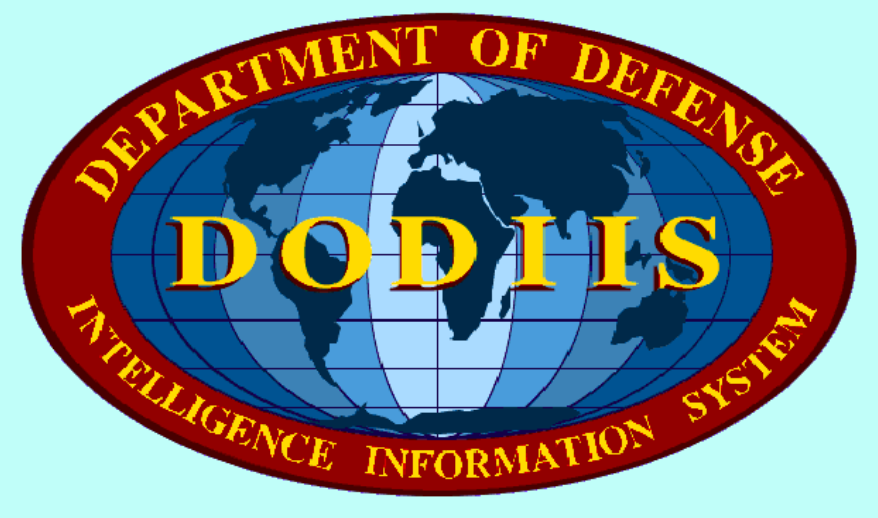


JOINT INTEGRATION TEST FACILITY (JITF)

DODIIS INTEGRATION

REQUIREMENTS and EVALUATION PROCEDURES

Version 2.1

October 7, 1999

Produced By:

Department of the Air Force
Air Force Research Lab
Rome Research Site
32 Brooks Road
Rome, New York 13441-4114

TABLE OF CONTENTS

SECTION 1

1. INTRODUCTION

This document specifies the requirements that Intelligence Mission Applications (IMAs) must meet in order to successfully integrate into the common operating environment defined by the Department of Defense Intelligence Information System (DODIIS). This environment emphasizes the objectives of integration, interoperability, shareable resources, and modularity of IMAs. The DODIIS IMA certification process has been defined to ensure that IMAs will operate in this environment. The tasking to Program Management Offices (PMOs) and identification of responsibilities for all phases of the certification process are specified in the *Department of Defense Intelligence Information System (DoDIIS) Instructions*.

The focus of integration testing is to verify that IMAs meet DODIIS requirements for functioning with existing infrastructures and resources. JITF testing verifies installation procedures and infrastructure compliance, identifies computer and network resource conflicts, and the operational impacts of applications cohabiting in a common environment. JITF testing validates that each application will function as a building block of the overall DODIIS.

The integration requirements contained in this document are organized by category:

- Documentation - These requirements evaluate the content and structure of IMA documents that the system administrator/installer will rely on to plan the IMA's resource requirements and to determine the effects of the software on the operational and security architectures of the site.
- Configuration and installation - These requirements evaluate the IMA installation process and the steps required to configure the IMA for use.
- Environment - These requirements evaluate the operating environment established or required by the IMA when it begins execution and the potential effects of that environment on other IMAs.
- Operation - These criteria examine aspects of the execution of the IMA that could affect the execution, configuration, or security of other IMAs, either on the same hardware platform or on other platforms at the site. Included in this category is how administration of the IMA integrates into the overall system administration strategy of a site.
- User Interface - These criteria are concerned with the integration of the IMA with the windowing system of the workstation.
- Security - These objectives identify areas of the design and operation of the IMA that may affect the site security architecture. These objectives may address areas of system security architecture that are not identified in the IMA security documentation.

This specification of DODIIS integration requirements consolidates into one document the requirements that were previously published in two JITF volumes, *Joint Integration Test Facility (JITF) Test Procedures, Volume 1, Infrastructure Compliance Testing* and *Joint Integration Test Facility (JITF) Test Procedures, Volume 2, Installation and Integration Scenario Testing*. A cross-index of earlier integration requirements to the current specification is included as an appendix to this document; the cross-index maps earlier requirements to current ones and identifies the document source of each requirement.

The integration requirements address integration of IMAs into client-server operating environments and also web-based multi-tiered operating environments. For this reason, a PMO may find that some requirements will not apply to the IMA because it was designed for one environment or the other.

The DODIIS community is in its initial planning for transition to the Defense Information Infrastructure Common Operating Environment (DII COE). There are many integration requirements that are common to both DODIIS and to DII COE. As transition planning matures, and the deliveries of IMAs compatible with DII COE are scheduled, this document will be updated to be compatible with the integration requirements of the DII COE.

This document is organized in the following sections:

Section 1 provides an introduction to integration requirements and additional information.

Section 2 provides a list of references.

Section 3 contains the DODIIS integration requirements, including explanations and test methods.

Two appendices are attached to this document: Appendix A contains a table of the DODIIS integration requirements and the cross-index to previous integration requirements. Appendix B contains a list of acronyms.

1.1 JITF INFORMATION

Comments and recommendations for changes to this document can be submitted by any reader and should be provided in writing. Please identify the page and paragraph associated with each comment. All written comments will be reviewed and a disposition for each comment will be provided to the originator of the comment. Comments can be submitted via the following means:

U.S. Mail: CUBIC CM
RL/IFEB
32 Brooks Rd
Rome, NY 13441-4114

Electronic Mail: cubic_cm@rl.af.mil

Additional copies of this document can be downloaded from the World Wide Web or Intelink at the following addresses:

Internet World Wide Web: http://www.if.afrl.af.mil/ programs/jitf

Intelink: http://web1.rome.ic.gov:82/vtf.cgi

1.2 CERTIFICATION CRITERIA FOR DODIIS INTEGRATION

Figure 1 illustrates the IMA certification process that is documented in the *DODIIS Instructions*, April 1999. JITF integration testing takes place during the IMA Independent Validation and Verification (IV&V) Process.

In accordance with the *DODIIS Instructions*, the JITF is tasked to make "go/no go" recommendations on IMAs to the DODIIS Management Board (DMB) as a result of integration testing.

A "no go" recommendation indicates that there are findings for the IMA under test that seriously affect the capability of the IMA to install and/or operate in a site environment without affecting other IMAs or site operations. The DMB is the decision authority for the certification process and uses the JITF recommendation in making a final determination for the IMA to proceed to the next phase.

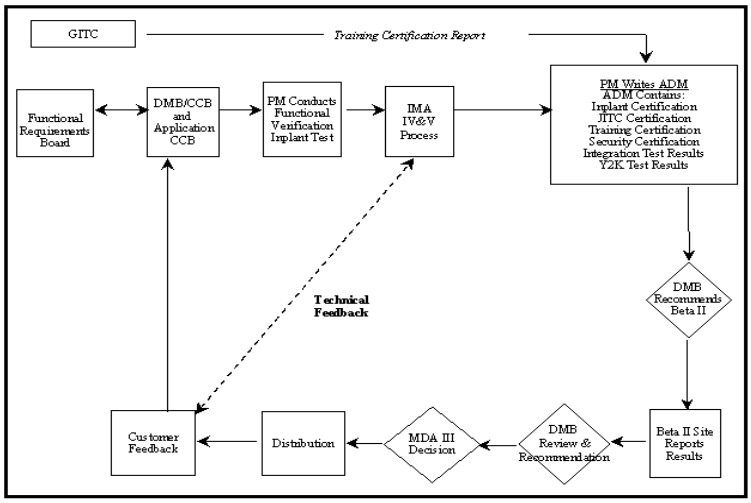


Figure 1 - IMA Certification Process

1.3 JITF TEST REPORTS

Test reports are available on the Virtual Test Folder (VTF) that is maintained by the JITF. The VTF is located on Intelink at http://web1.rome.ic.gov:82/vtf.cgi. The JITF test report details the extent of compliance with the DODIIS integration requirements and provides an assessment of the consequences of the resulting level of integration quality of the IMA.

Criteria for successful evaluation of IMA integration in the IMA IV&V process phase of the certification process are grouped in the following categories:

- Integration Quality
- Adherence to DODIIS Architecture
- Documentation
- Adherence to IMA Certification Process

For each category, the JITF identifies and reports specific findings. The findings are analyzed to determine the effect each finding will have on the overall quality of the IMA. The evaluation of Integration Quality is based on the integration requirements specified in this document.

The findings and recommendation for each IMA are published in the JITF Test Report. The JITF Test Report for the IMA under test will include:

- Evaluation of compliance with the DODIIS integration requirements
- Assessment of effects of non-compliance with integration requirements
- Recommendations on integration security issues
- Identification and assessment of other issues that affect the usability of the system baseline in operational environments
- "Go/no go" recommendation for continued movement of the IMA through the IMA certification process

1.4 IMPACT CODE LEVELS FOR JITF INTEGRATION TESTING

The JITF evaluates the extent to which the IMA meets each requirement. For each requirement not met by the mission application, the JITF documents a test finding and assesses an Impact Code level for that finding. The impact code is a measure of the significance of the finding with respect to integrating the IMA into site architecture.

Not all of the integration requirements have equal weight. That is, the failure to meet some requirements has more significance than the failure to meet other requirements. In addition, the design of the IMA will also influence the significance of requirements that are not met.

A successful evaluation means that the mission application has passed integration testing, and the JITF will recommend that the IMA proceed to the next step in the DODIIS IMA certification process.

An unsuccessful evaluation means that the IMA has failed integration testing, and the JITF will recommend that the IMA not proceed to the next step in the DODIIS IMA certification process.

The following codes are used by JITF test teams to indicate the severity or significance of each integration finding.

Impact Code 1

A finding that, without resolution, either

a) prevents either the IMA or another application or component of the infrastructure from operating properly;
b) creates a security vulnerability in the IMA or site architecture that can be exploited by a general user without taking advantage of other vulnerabilities or capabilities; or
c) seriously increases the level of effort of site personnel to manage and/or use the IMA or other applications.

An Impact Code 1 finding is assigned if the IMA baseline must be changed in order to continue testing, if the resolution requires an excessive level of effort, or if the resolution introduces additional problems in the installation or operation of the application.

The level of effort is a key determinant for Impact Code 1 findings. The time or expertise that is required to install, manage, or use the application cannot exceed what is reasonably expected for an IMA. For example, if the installation guide says that the IMA can be installed in a single day, but the installation takes more than 20 working hours, then an Impact Code 1 can be appropriately applied.

Impact Code 2

A finding that, without resolution,

a) has a significant effect on the operation of either the mission application or on another application or component of the infrastructure; or
b) creates a security vulnerability in the IMA or site architecture that could be exploited by a general user only if the user is able to take advantage of other vulnerabilities or capabilities not typically available to him or her.

The finding can be temporarily resolved by a change in procedure or configuration. The successful resolution requires technical expertise that is not expected of general users, or the resolution requires a significant level of effort by site administrators. The resolution does not cause significant delay in integration testing; instead, it can be proposed and evaluated during integration testing at the JITF.

Impact Code 2 findings may cause integration test failures depending upon the level of effort required to implement the resolution (and the confidence in it). An Impact Code 2 problem may

be elevated to an Impact Code 1 if proposed resolutions either do not work successfully or produce additional Impact Code 2 and 3 findings.

Impact Code 3

A finding that, without resolution, has a significant effect on the operation of either the IMA or on another application or component of the infrastructure. The finding can be temporarily resolved by a change in procedure or configuration. The successful resolution does not require technical expertise that is not expected of general users, or the resolution does not require a significant level of effort by site administrators. The resolution does not cause significant delay in integration testing; instead, it can be proposed and evaluated during integration testing at the JITF.

Impact Code 3 findings do not cause integration test failure, but the accumulation of Impact Code 3 findings may affect the JITF's "go/no go" recommendation.

Impact Code 4

A finding that does not significantly affect the operation of the IMA or another application or component of the infrastructure. The finding can be resolved by a workaround that can be implemented as a change in procedure or configuration during integration testing without a significant level of effort, or the finding can be left as is. Even though the finding has some affect on the configuration or operation of the mission application or of other components of the site architecture, the general user will be able to perform mission functions, and the administrator will be able to manage the mission application. Findings in this category are of lesser importance, but the accumulation of Impact Code 4 findings may affect the JITF's "go/no go" recommendation.

SECTION 2

2. REFERENCES

AIA 497th Intelligence Group /INDS, *Test and Evaluation Policy for Department of Defense Intelligence Information System (DoDIIS) Intelligence Mission Applications (IMA),* April 1999

Defense Information Systems Agency, *Department of Defense Joint Technical Architecture,* Version 3.0 Draft 1, 26 February 1999

DODIIS Management Board, *DODIIS Developer's Guide for Automated Information Systems (AIS) Security in DoD Intelligence Information Systems*, November 1993.

DODIIS Management Board, *DODIIS Instructions*, January 1999.

DODIIS Management Board, *Department of Defense Intelligence Information System (DODIIS) Security Architecture Guidance and Directions*, February 1995.

Joint Interoperability and Engineering Organization Defense Information Systems Agency *Defense Information Infrastructure (DII) Common Operating Environment (COE) Integration and Runtime Specification (I&RTS) v3.1*, October 1998.

Joint Interoperability and Engineering Organization, Defense Information Systems Agency *User Interface Specifications for the Defense Information Infrastructure (DII) Version 3.0* February 1998.

Microsoft Corporation, *Designed for Microsoft® Windows NT® 4.0 and Windows® 98 Logo, Handbook for Software Applications, Version 3.0d*, February 4, 1999

Rome Laboratory RL/IRDO/JITF *DODIIS CSE Integration Objectives And Evaluation Procedures DRAFT* 2 October 1996.

Readers who are interested in the original guidelines for the DODIIS infrastructure and tasking of the Joint Integration Test Facility should examine the following documents.

AIA 497 IG, *Department of Defense Intelligence Information System (DODIIS) Client-Server Environment (CSE) Specification,* June 1992.

AIA 497 IG, *DODIIS Client-Server Environment System Services (CSE-SS) Requirements,* February 1994.

DODIIS Management Board, *DODIIS Mission Systems Instructions to DExAs, PMOs, and Developers*, February 1997.

Rome Laboratory RL/IRDO/JITF *Joint Integration Test Facility (JITF) Test Procedures, Volume 1 Infrastructure Compliance Testing*, 18 June 1997.

Rome Laboratory RL/IRDO/JITF *Joint Integration Test Facility (JITF) Test Procedures, Volume 2, Installation and Integration Scenario Testing*, 18 June 1997.

Rome Laboratory RL/IRDO/JITF *Concept of Operations for the DODIIS Joint Integration Test Facility (DODIIS JITF) at Rome Laboratory*, 4 April 1996.

SECTION 3

3. DODIIS INTEGRATION REQUIREMENTS

Requirements for integration are listed and described in this section. For each requirement an explanation is provided as needed and the evaluation method is listed. The method selected to verify compliance with the integration requirements depends upon the requirement being evaluated; where possible, evaluation of requirements is automated through the use of software testing tools developed or acquired by the JITF.

A reference summary of the integration compliance requirements is included as Appendix A. The appendix includes a cross-index that maps each integration requirement to integration requirements identified in previous JITF test and evaluation procedure documents.

3.1 DOCUMENTATION

DOC-1 IMA documents shall contain page numbers for all sections and appendices.

REQUIREMENT CLARIFICATION	TEST METHOD
Page numbering improves the utility of each IMA document. This can be especially significant when the reader must identify to a third party (such as a help desk) an entry in a document that either has errors or is unclear.	Application documents will be inspected for inclusion of page numbers.

DOC-2 IMA documents shall contain numbered sections.

REQUIREMENT CLARIFICATION	TEST METHOD
Construction of a document in numbered sections improves the utility of the document and aids the reader in identifying areas with errors or requiring clarification.	Application documents will be inspected for inclusion of numbered sections.

DOC-3 Figures and tables in IMA documents shall have titles and reference numbers.

REQUIREMENT CLARIFICATION	TEST METHOD
Assigning titles and reference numbers to all figures and tables improves the utility and readability of the document.	Application documents will be inspected for inclusion of titles and reference numbers on all figures and tables.

DOC-4 Soft copy documents shall match hard copy versions in content, structure, and sectioning.

REQUIREMENT CLARIFICATION	TEST METHOD
In order to avoid confusion that may occur when matching a soft copy version of a document to a hard copy version (e.g., when discussing a problem with the IMA help desk), the two versions should match exactly. At a minimum, the content, structure, and sectioning of the document should be consistent for both versions.	The soft copy version will be compared to the hard copy version. This objective is met if the content, structure, and sectioning of the soft copy document match the sectioning of the hard copy document.

DOC-5 IMA configuration and installation information shall be consolidated into a single configuration and installation document.

REQUIREMENT CLARIFICATION	TEST METHOD
The IMA administrator/installer must be able to find all necessary information for the installation of the IMA in a single, logically ordered, document. This approach lowers the probability of errors during the configuration and installation process. If configuration and installation instructions must be spread beyond a single document, then these documents must specifically reference the parts needed in each other, preferably by section and/or step.	The objective will be evaluated by inspection of the configuration and installation guide. This objective is not met if the configuration and installation information is spread across several documents and the references to additional documents are not explicitly stated.

DOC-6 The IMA configuration and installation guide shall include installation verification information.

REQUIREMENT CLARIFICATION	TEST METHOD
Configuration and installation of the IMA can directly affect the operating and security architectures of the IMA itself and of the site. The JITF will confirm that the IMA was successfully installed and configured according to the IMA baseline. Verification documentation assists the JITF, as it would a DODIIS site, with this confirmation.	Acceptable verification documentation includes: • System Test Plan and Procedures • System Security Test Plan and Procedures Site Acceptance Test (SAT) Plan and Procedures, or similar documents • The objective is met if verification documentation is provided. The evaluation will include an estimation of the adequacy of the verification documentation.

DOC-7 The IMA configuration and installation guide shall specify if the IMA requires a dedicated platform for the IMA server or if the IMA server can be installed on a platform shared with other IMA servers.

REQUIREMENT CLARIFICATION	TEST METHOD
One goal of the DODIIS architecture is to give the sites flexibility in selecting how each IMA will be installed and used. An IMA that, by design, permits sharing of a platform with other IMA servers allows sites to select platforms based upon IMA performance and resource usage. An IMA that, by design, requires a dedicated platform may hinder integration of the IMA into a site simply because the site is forced to acquire and install hardware and extend its IMA administration strategy to cover the newly installed IMA. There are risks associated with both approaches. The extent of the risk with regard to site integration depends upon the quality of the IMA configuration and installation guide and on availability of resources and personnel to install and manage the IMA.	Application configuration and installation guide will be inspected to verify that the need for a dedicated server platform or the ability to share a server platform is specified. The absence of this information causes the IMA to not meet this requirement.

DOC-8 The IMA installation and configuration guide shall contain step by step instructions to perform IMA installation and configuration.

REQUIREMENT CLARIFICATION	TEST METHOD
The goal of IMA configuration and installation guide is to permit the reader (e.g., the IMA administrator) to install and configure the IMA without error. The configuration and installation guide should not increase the probability of error due to lack of clarity.	Installation and configuration guide will be inspected for step by step instructions. Each step should be concise and constitute a single action. The step should be explained sufficiently to avoid unnecessary guesswork or presumptive decisions by the installer.

DOC-9 The IMA configuration and installation guide shall include instructions to add the IMA to the infrastructure application selection mechanism.

REQUIREMENT CLARIFICATION	TEST METHOD
The installation process must include the steps to add the IMA to the application selection mechanism (e.g., background window menu IMA folder, etc.). The installation procedure provided by the IMA developer must include the IMA name, executable location, and the command lines that are required to set needed environment variables and launch the IMA.	The IMA configuration and installation guide will be examined to verify that instructions for adding the IMA to the infrastructure application selection mechanism are included. Once the installation has been completed, the application selection mechanism (e.g., background window menu) will be invoked on the test workstation. Verify that an entry for the IMA appears in the menu as documented in the installation procedures. Select the IMA from the background menu and verify the execution of the IMA.

DOC-10 IMA documentation shall specify points of contact (phone, electronic mail, etc) for IMA support.

REQUIREMENT CLARIFICATION	TEST METHOD
Administrators and users must be able to identify and communicate with personnel who can assist with questions and problems. Telephone and electronic mail are acceptable forms of communication; however, the PMO should consider that unclassified communication may not be	Application documents will be inspected to verify that points of contact are provided. The information must include the office or organization name, telephone number (s), and electronic mail address, if one is available.

possible for DODIIS users.	

DOC-11 The IMA configuration and installation guide shall specify the minimum amount of disk space needed to install and execute the IMA.

REQUIREMENT CLARIFICATION	TEST METHOD
All space requirements needed to install and run the IMA must be specified. This includes disk space for executables, as well as storage for IMA and user data.	Configuration and installation guide will be inspected to verify that recommended disk space is specified.

DOC-12 The IMA configuration and installation guide shall specify the name(s) and size(s) of file system(s) that are required to install and execute the IMA.

REQUIREMENT CLARIFICATION	TEST METHOD
Some IMAs may require or recommend specific file systems for technical reasons such as raw partitions for data base servers. In such cases, the file systems and required sizes must be stated. The need for specific file names must be weighed against the impact of the IMA installation to the site's architecture. Names should be arbitrary, and selection of names should be left to the site administrator.	Configuration and installation guide will be inspected to verify that required file systems and sizes are specified. Specific file system names (if required) will be stated. The configuration and installation guide must specify all space required for each major directory that the IMA copies files to. For example, if the IMA installs files in the /etc/rc3.d directory, the space required in that directory must be specified. For NT, if an application can be installed on a file system other than the Windows Root drive, the space required on that file system, as well as the space required in the Windows Root drive, must be specified. This requirement applies to both UNIX file systems and to Windows NT disks (e.g., requiring software loading onto a specific disk). The requirement is Not Applicable if the IMA does not require specific configuration of file systems.

DOC-13 The IMA configuration and installation guide shall specify the recommended and minimum size of random access memory (RAM) required to execute the IMA.

REQUIREMENT CLARIFICATION	TEST METHOD
This is typically a performance issue; IMAs should make recommendations on RAM for site consideration. Both recommended and minimum RAM sizes should be specified. These specifications should be made for both user workstations and IMA server platforms.	Configuration and installation guide will be inspected to verify that recommended and minimum RAM size is specified.

DOC-14 The IMA configuration and installation guide shall specify the operating system versions and operating system packages/subsets that must be installed to support the IMA.

REQUIREMENT CLARIFICATION	TEST METHOD
The IMA should not require that each site install the full operating system load as routine practice. Therefore, the IMA should identify the software dependencies with regard to specific operating system version and also the operating system modules (i.e., subset packages or resource packs) that must be installed in order for the IMA to operate properly.	Configuration and installation guide will be inspected to verify that operating system versions and packages/subsets/resource packs are specified.

DOC-15 The IMA configuration and installation guide shall specify the operating system patch levels that must be installed to support the IMA.

REQUIREMENT CLARIFICATION	TEST METHOD
IMA developers make independent decisions regarding patch level compatibility. Therefore, the Configuration and installation guide must state known dependencies upon patch levels. This may not be a significant issue for sites that stay	Configuration and installation guide will be inspected to verify that patch levels for each supported operating system are specified. The requirement is met if the specific patch list is provided; it is not sufficient to simply require "the latest patches".

current with all operating system packages. However, it is necessary information for sites that may not be current and is an incentive for site administrators to update patch levels on site workstations. The documentation shall include information as to what OS patches may be required.	

DOC-16 The IMA configuration and installation guide shall specify any modifications made to the operating system configuration that are required to support the IMA.

REQUIREMENT CLARIFICATION	TEST METHOD
Modifications to the Unix kernel or to the NT operating system configuration are not necessary for most IMAs. Modification would be required if the IMA requires an additional hardware device, additional software resources such as interprocess communication, or additional drivers for I/O devices. In such situations, the necessary modifications must be clearly stated in the configuration and installation documentation.	Configuration and installation guide will be inspected to verify that modifications for each supported operating system are specified. This requirement is Not Applicable if no modifications are required.

DOC-17 The IMA configuration and installation guide shall specify additional hardware and associated drivers that are required to support the IMA.

REQUIREMENT CLARIFICATION	TEST METHOD
If the IMA requires additional hardware and installation of software drivers to control the hardware, the configuration and installation guide will clearly specify the steps needed to successfully install and configure both.	Configuration and installation guide will be inspected to verify that instructions to install additional hardware and associated software drivers in each supported operating system are specified. If no additional hardware and installation of software drivers to control the

	hardware are utilized, this requirement is Not Applicable.

DOC-18 The IMA configuration and installation guide shall specify additions/modifications to system configuration files that are required to support the IMA.

REQUIREMENT CLARIFICATION	TEST METHOD
Many IMAs may use system configuration files. As a result, no IMA should make undocumented changes to configuration files.	The IMA configuration and installation guide should clearly specify the modifications that will be made during installation. The installation process must not overwrite system configuration files (e.g., /etc/hosts, /etc/services, and /etc/syslog.conf), since information that was added by other IMAs may be lost. Instead, the IMA should add entries to the existing files. For the NT platform, documentation must clearly specify the settings for computer peripherals that are required by the IMA. No undocumented changes to the NT Registry, Windows.ini, System.ini, Config.sys, or Autoexec.bat files shall be made. Review the configuration and installation guide to verify that all modifications to IMA configuration files are specified.

DOC-19 The IMA configuration and installation guide shall provide rules defining appropriate file ownerships and permissions for all files and directories that are loaded or modified during IMA installation.

REQUIREMENT CLARIFICATION	TEST METHOD
IMA documentation should include information on file ownerships and permissions. This is needed to permit the security officer or administrator to confirm that all ownerships and permissions are set correctly during installation. The information must be included even if the	The appropriate IMA documentation, e.g., Configuration and Installation Guide, Version Description Document (VDD), will be examined for the inclusion of file ownerships and permissions for all files created or modified during configuration and installation of the IMA.

installation is completely automated.	

DOC-20 The IMA configuration and installation guide shall specify the audit configurations (i.e., audit flags, etc.) that must be set in order to meet the IMA security requirements.

REQUIREMENT CLARIFICATION	TEST METHOD
DODIIS security policy permits IMAs to rely on the underlying operating system audit function for auditing of IMA activity. For such IMAs, the Configuration and installation guide must clearly specify the audit flags that must be set in order to meet the IMA's security concept of operations.	Configuration and installation guide will be inspected to verify that audit flags for each supported operating system are specified.

DOC-21 The IMA configuration and installation guide shall identify other software products on which the normal operation of the IMA is dependent.

REQUIREMENT CLARIFICATION	TEST METHOD
Even simple IMAs may depend upon the presence and operation of third party software. This typically is true for IMAs that rely on data base management systems or on word processing systems. In each case where the IMA depends upon the presence and operation of third party software, the configuration and installation guide will clearly state the identity of the software, the version and patch level of the software, and the nature of the dependency.	IMA configuration and installation guide will state the name, version, and patch level of other software on which the IMA depends. The nature of each dependency will be stated.

DOC-22 Comprehensive instructions shall be provided for uninstalling the IMA, including backing out of a failed installation so that it can be reinstalled.

REQUIREMENT CLARIFICATION	TEST METHOD

Operator errors or script problems may cause the IMA installation to fail and thus require a partial or total rollback of the installation. Mission IMA installation should not be like a black box with respect to determining exactly which portions may have been installed before a failure occurred. Additionally, the initial point of failure may not be detected. This means the installation may continue even after part of the installation has failed. The error may be discovered, or the whole installation may fail. During this time, additional undetected errors may occur as consequences of the original error. The residue left from the failed attempt may cause conflicts during the next installation attempt. Without instructions to back out of the installation, the only way to fully insure a clean reinstallation may be to install the entire IMA from the operating system up. This should be avoided. The installation and rollback strategy should be designed so that the installation would only be rolled back to the point of failure or to the beginning of the segment or module where the error occurred.	The objective will be met by inclusion of rollback instructions in the configuration and installation documentation.

DOC-23 IMA documentation shall specify the browsers and browser versions that are compatible with the IMA.

REQUIREMENT CLARIFICATION	TEST METHOD
IMA s should test against browser versions that are currently in use in the DODIIS community (i.e., not only the latest versions). The IMA documentation should state which browsers are known to be compatible with the IMA.	IMA documentation will be inspected to verify that compatible browsers are identified. This requirement is Not Applicable if the IMA does not use a browser.

DOC-24 The IMA configuration and installation guide shall specify any browser settings that are necessary to access the IMA.

REQUIREMENT CLARIFICATION	TEST METHOD
IMA s should not assume specific browser settings because site policy may dictate browser configuration. However, if there are configuration settings that are necessary (e.g., Java enabled), the Configuration and installation guide must identify them.	IMA documentation will be inspected to verify that necessary browser settings are identified. This requirement is Not Applicable if the IMA does not use a browser.

DOC-25 If the IMA design requires the use of plug-ins, the IMA documentation shall include a list of required browser plug-ins, the source of the plug-ins and appropriate licenses, and DMB approval to use the plug-ins.

REQUIREMENT CLARIFICATION	TEST METHOD
Since access to browser plug-ins is extremely limited on classified networks, the administrator or user must be notified before the IMA is used that a plug-in is necessary. Therefore, the configuration and installation guide must list the plug-ins that are required and how the plug-ins and licenses (if required) can be obtained. Since downloading and installing a plug-in may have security implications, DODIIS security policy requires that the DMB approve the use of the plug-in. This approval must be documented in the configuration and installation guide set provided to the JITF.	IMA documentation will be inspected to identify the required plug-ins and the sources for each plug-in. The documents will also be inspected for documentation of DMB approval to use the plug-in. The documentation must also include instructions to install and configure the plug-ins. In most cases, configuration and installation is performed automatically by the browser; any additional manual steps must be included in the documentation. This requirement is Not Applicable if the IMA does not use a browser.

DOC-26 If the IMA design includes implementation of JAVA applets, the IMA documentation shall include documentation of IMA server registration with Intelink Central, documentation of JAVA applet registration with Intelink Central, and documentation of results of JAVA applet code review.

REQUIREMENT CLARIFICATION	TEST METHOD
DODIIS policy requires written documentation of the registration and code review of JAVA applets. For any application that implements JAVA applets, the documentation specified in this requirement is mandatory. If the documentation is not provided to the JITF, the JITF must forward to the DMB a "no go" recommendation on the basis of this deficiency. The DODIIS Instructions do not specifically state which organization is responsible for reviewing JAVA applet source code. The code review can be done by the security certifiers or a third party organization. It is the responsibility of the PMO to arrange code review.	The IMA documentation will be inspected to determine if JAVA applets are implemented. JAVA applets are permitted to be hosted only on servers that are registered with Intelink Central. The server registration process does not produce written confirmation. Proof of registration is demonstration by the listing of the mission application server on the Intelink Central Home Page. The registration of JAVA applets can be done on-line with Intelink Central. Copies of the registration forms can be included with the mission application documentation as documentation of registration. Documentation of applet code review must include the date of the review, name and address of the reviewer(s), and all findings from the review. This requirement is Not Applicable if the IMA does not use a browser.

DOC-27 The IMA configuration and installation guide shall specify the network address and port number for proxy server(s) if required to access the IMA web server.

REQUIREMENT CLARIFICATION	TEST METHOD
The use of network firewalls will increase in the DODIIS	IMA documentation will be inspected to verify that the address and port

community. Proxy servers are used to permit certain types of traffic (e.g., web traffic to pass the firewall boundary without interception). IMAs that maintain a central server (or set of servers) for access by clients throughout the DODIIS community must inform sites of the address and port number of the proxy server in order to access the IMA server. Therefore, this information must be included in the configuration and installation guide.	number of the proxy server (if present) is included with the configuration and installation information. This requirement is Not Applicable if the IMA does not use a browser.

DOC-28 The IMA documentation shall specify Uniform Resource Locator (URL) for access to the IMA as a logical hostname that can be resolved by the site's name resolution service.

REQUIREMENT CLARIFICATION	TEST METHOD
The URL is necessary in order to access the IMA server. It must be specified in the user documentation as a logical host name rather than as a numeric Internet Protocol (IP) address.	IMA documentation will be inspected to verify that the IMA URL is specified as a logical hostname. This requirement is Not Applicable if the IMA does not use a browser

DOC-29 IMA design documentation shall specify if secure HTTPS connections are required.

REQUIREMENT CLARIFICATION	TEST METHOD
Most currently used browsers support secure Hyper Text Transfer Protocol (http) communication. This requirement simply states that the need for secure http communication should be identified in the design documentation.	IMA design documentation will be inspected to verify that the requirement for secure http communication is stated. If the IMA does not use a browser this requirement is Not Applicable.

DOC-30 IMA design documentation shall specify the standards implemented by the IMA that are mandated by the Joint Technical Architecture (JTA).

REQUIREMENT CLARIFICATION	TEST METHOD

The JTA establishes the minimum set of rules governing information technology within Department of Defense systems. The scope includes standards for information-processing, information-transfer, the structure of information and data, human-computer interface standards for information entry and display, and information-system security standards. Information technology includes any equipment or interconnected system or subsystem of equipment used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. The JTA mandates the minimum set of standards and guidelines for the acquisition of all DoD systems that produce, use, or exchange information. The JTA must be used by anyone involved in the management, development, or acquisition of new or improved systems within the Department of Defense. The DODIIS Instructions mandate that the acquisition and development of IMAs comply with the standards specified by the JTA. At this time, evaluation of actual implementation of and compliance with JTA standards is beyond the scope and resources of the JITF. As a minimum, the IMA documentation shall identify the services area(s) that are addressed by the IMA functional design and shall identify in the IMA design documentation the appropriate standards mandated by the JTA that are implemented by the IMA..	IMA design documentation will be inspected to verify that the following items are included: 1. Identification of the services areas as specified in the Joint Technical Architecture that the IMA addresses. 2. Specification (i.e., references) of each standard that is implemented by the IMA and that is mandated by the JTA for each service area addressed by the IMA. This requirement is met if the IMA implements only standards included in the JTA. The IMA can implement standards that are not included in the JTA if there is no corresponding standard in the JTA that performs the same functions. If the JTA does not implement JTA standards, the design documentation must specify either that the IMA has received approval from the DMB to implement another standard and documents that approval, or that there is no JTA standard that implements the required functions. Otherwise, the requirement is not met.

3.2 INSTALLATION AND CONFIGURATION

INST-1 IMA installation shall not require installation of the operating system.

REQUIREMENT CLARIFICATION	TEST METHOD
In accordance with the integration methodology developed by the DODIIS community, installing the IMA can and should be done on a previously installed and executing operating system. There should be no requirement to reload the operating system simply to install another IMA. Additional packages/ subsets/resource packs can be added to the operating systems, and the operating system configuration can be modified without requiring a new installation of the operating system. Reloading the operating system means the rest of the system (i.e., other IMAs) must be backed up and restored. This is a time consuming process, particularly if many workstations in the site are affected.	The objective is not met if the configuration and installation documentation calls for an operating system reload or if the IMA's configuration and installation scripts reload the operating system. If the actual installation of the IMA cannot be successfully completed without reloading the operating system, then the objective is not met.

INST-2 IMA installation shall not require reinstallation of currently loaded COTS or GOTS applications.

REQUIREMENT CLARIFICATION	TEST METHOD
The IMA may require the use of an earlier or later version of currently installed software. This does not necessarily violate the objective. The key point in this requirement is that the installation of the IMA must not assume or otherwise require reinstallation of current applications. If the required version of a key application is already present, then the installation should proceed.	The installation process will be monitored for the installation of COTS and GOTS software. The objective is not met if installed software matches the release and version of previously installed software and installs without prompting the user or if the installation process automatically installs additional COTS or GOTS software without checking if the software is already present.

INST-3 The IMA shall not include bundled support applications.

REQUIREMENT CLARIFICATION	TEST METHOD
Support applications are software that are commonly used by either other applications or users. This includes word processors, spread sheets, browsers, and file transfer utilities. These applications are typically provided by a component of the infrastructure. Since these applications are for general use, the IMA design can assume that necessary support applications are either present or can be readily installed. In some cases, it may be reasonable to bundle third party software in the IMA installation. This decision should be based on the general utility of the third party software, the cost and ease of procuring that software, and the probability that the site may already possess the software. In all cases, the installation should not force the installation of the bundled software, particularly if the software has been previously installed via another source. A reasonable approach is that the administrator is queried during the installation process whether the software should be installed.	The appropriate IMA documentation (e.g., Configuration and Installation Guide, VDD) will be examined to determine if support applications are included in the distribution of the IMA. Following the installation of the IMA, all directories that have been touched by the installation process will be examined to determine if any support applications have been loaded or overwritten. Verify that support applications are NOT bundled with the installed IMA. Examine the IMA directory tree and execute the command: Unix: *ls –latR* NT: *dir /s* Examine appropriate directories to determine if any support applications have been loaded or overwritten. For each support application that is found, the finding must list the application and its normal source of availability (e.g., Intelink for a browser utility) so that the IMA installation will be able to specify where to obtain the application.

INST-4 The IMA shall not include bundled implementations of any standard network protocol.

REQUIREMENT CLARIFICATION	TEST METHOD
Since network protocols and services are provided by the DODIIS infrastructure, it is outside the scope of IMAs to	Verify that the IMA design does not bundle any implementation of standard network protocols. After configuration and installation of the IMA,

bundle them within their own products. Instead, the IMA must use the application program interfaces provided by the infrastructure. This prevents the inclusion of redundant and potentially non-interoperable software into the site-operating environment and reduces the amount of IMA software that must be managed. This requirement applies to the use of any network protocol, including Transmission Control Protocol (TCP)/IP and low-speed network communications such as the following: - file transfer protocol - telnet protocol - mail protocols - routing protocol - remote procedure communication (e.g., Remote Procedure Call (RPC)) - windowing protocols (e.g., X11)	directories (both system directories and directories owned by the IMA) that have been accessed during the installation of the IMA will be examined to verify that no network protocol software has been installed. For each directory that was accessed during installation, examine the directory tree and review files (i.e., x-ftp, ftp, etc.) by executing the command: Unix: *ls –latR* NT: *dir /s* Verify that the IMA design and installation does not include bundled implementations of any standard network protocol by inspecting these files.

INST-5 IMA installation design shall support installation on user workstations and on application servers for export to user workstations.

REQUIREMENT CLARIFICATION	**TEST METHOD**
One goal of the DODIIS infrastructure is to permit sites to allocate their computing resources according to their needs rather than according to the design of individual IMAs. An IMA should be designed so that a site can install it on individual workstations or on an application server. The IMA design should not require a specific approach.	Using the IMA installation instructions, the IMA will be loaded on a user workstation. Once the installation is complete, test cases from the IMA test procedures will be executed to demonstrate the successful execution of the IMA. Using the IMA installation instructions, the IMA will be loaded on an application server. The IMA will be exported for execution by user workstations. Following installation of the IMA test cases from the IMA test

	procedures will be executed to demonstrate execution of the IMA on user workstations.

INST-6 IMA shall not modify the native programming utilities and libraries.

REQUIREMENT CLARIFICATION	TEST METHOD
In order to increase the portability of IMAs and to simplify the installation and management of IMAs, the infrastructure services that are available to IMAs must be kept stable. Since the infrastructure will provide a common set of services and functions to all IMAs, an IMA must not replace or modify parts of the underlying operating system or software run-time environment.	After configuration and installation of the IMA, the state (i.e., modification time, ownership, etc.) of the directories containing programming utilities and libraries will be compared to the state of these same directories before the IMA was installed. It is not acceptable for the IMA to install a library that is a duplicate of a system library. On Unix platforms check the IMA utilities and library directories by executing the following commands and noting the modification date on each library: *sh* *for i in /bin /usr/bin/sbin/usr/sbin/usr/openwin/bin/usr/ucb/usr/etc/lib /usr/lib * */usr/openwin/lib /etc/lib /etc/security/lib* *do* *echo Checking directory $i* *ls -latR $i* *done* On NT platforms check the IMA utilities and library directories by executing Analyzer tool.

INST-7 The IMA shall not require modification of networking protocols or services.

REQUIREMENT CLARIFICATION	TEST METHOD

Since network protocols and services are infrastructure services, they are not "owned" by any IMA. Therefore, modification of these services is not permitted. This requirement also covers dependencies of the IMA on services such as NIS and NIS+ on UNIX platforms. The selection of such a service is a site choice; the IMA cannot dictate which service the site can use or force the site to modify the network information service configuration of client and server systems. Instead, the IMA should be designed to operate with either service running or with none running. An IMA that explicitly requires the use of NIS rather than being capable of operating under NIS or NIS+ will fail this requirement.	After configuration and installation of the IMA, the state (i.e., modification time, ownership, etc.) of the directories containing the networking protocol and services will be compared to the state of these same directories before the IMA was installed. The networking services are found within the standard IMA directories. Check to see if inetd is configured to start a process differently from the IMA process for a given service or if the IMA has added a new, non-standard service by executing the command: **NIS+:** *ls -l /etc/services* If the time indicates that the file has been modified during the installation, execute the command: *cat /etc/services* Continue by executing the command: *cd /var/nis/data or cd /var/nis/<hostname>* *ls -l services.org_dir.log* If the time indicates that the file has been modified during the installation, execute the command: *niscat services.org_dir* **NIS:** *ls -l /etc/services* If the time indicates that the file has been modified during the installation, execute the command: *cat /etc/services* Continue by executing the command: *cd /var/yp/src* *ls -l services* If the time indicates that the file has been modified during the installation,

	execute the command: *ypcat services* **LOCAL:** *ls -l /etc/services* If the time indicates that the file has been modified during the installation, execute the command: *cat /etc/service*s On Solaris platforms, verify that the "nsswitch.conf" file has not been altered as a result of the IMA installation. Compare the contents of the /etc/nsswitch.conf file before installation of the IMA to /etc/nsswitch.conf after installation. There should be no changes to the file.

INST-8 The IMA software and documentation shall explicitly identify the software version and release of IMA in both documentation and software.

REQUIREMENT CLARIFICATION	TEST METHOD
A DODIIS site must be able to exactly identify what it is installing and configuring in order to ensure that the software is current. This information ensures that the documentation and software are for the same version and release. This information is also necessary when reporting errors or problems to a software support facility or help desk.	This objective will be evaluated by inspection of the software and documentation for version and release numbers. The information from both sources must match. Software items to examine include Splash Screens, About dialog box, and Help.

INST-9 The IMA can be un-installed using instructions provided in IMA configuration and installation guide.

REQUIREMENT CLARIFICATION	TEST METHOD
Operator errors or script problems may cause the IMA installation to fail and thus require a partial or total rollback	During installation of the IMA, the test engineers will record if the installation creates backup copies of system configuration files that are modified by the

of the installation. IMA installation should not be like a black box with respect to determining exactly which portions may have been installed before a failure occurred. Additionally, the initial point of failure may not be detected. This means the installation may continue even after part of the installation has failed. The error may be discovered, or the whole installation may fail. During this time, additional undetected errors may occur as consequences of the original error. The residue left from the failed attempt may cause conflicts during the next installation attempt. Without instructions to back out of the installation, the only way to fully insure a clean reinstallation may be to install the entire IMA from the operating system up. This is a drastic step that should be avoided. The installation and rollback strategy should be designed so that the installation would only be rolled back to the point of failure or to the beginning of the segment or module where the error occurred.	installation process. Configuration and installation of the IMA will use incorrect data and/or script errors to induce appropriate installation failures. Following the installation failure, the IMA will be un-installed using the instructions provided in IMA documentation. The requirement is met if the IMA can be un-installed successfully, and the installation of the IMA can be successfully restarted and completed. If testing time is available and circumstances permit, after the IMA has been successfully installed, the IMA will be un-installed by following the instructions in the IMA documentation. The requirement is met if the system is restored to the state existing before the IMA was initially installed. This includes recovery of all modified files, deletion of any file systems that were created during the IMA installation, and removal of any system configuration changes that were made during IMA configuration.

INST-10 The IMA installer shall not be required to make changes to installation scripts as part of the installation process.

REQUIREMENT CLARIFICATION	TEST METHOD
Installation scripts are part of the IMA baseline. Direct installer modification of configuration and installation scripts violate the concept of a frozen software baseline. IMAs should be designed for site integration with choices performed by logical operators like “if” and “case” statements instead of requiring the installer to modify the script code at each site. This is especially true for logical choices involving the various operating systems supported by	The requirement will be verified during configuration and installation of the IMA. The requirement is essentially not met if any installation script is opened for editing and any edits are saved. Changes to any installation scripts that are required for the configuration and installation to be successfully completed will be recorded by the JITF. Changes include adding or modifying environment variable declarations, modifying file and directory paths, correcting typographical errors, and modifying script logic.

the IMA. If physical changes must be made to the scripts at end sites, the changes should be generated by other code, which is included in the software baseline.	

INST-11 The IMA installer shall not be required to enter extraneous or superfluous information during installation.

REQUIREMENT CLARIFICATION	TEST METHOD
Software modules can often be reused in environments and contexts other than their original purposes. Software reuse is highly recommended and promoted by the DODIIS IMA integration methodology. Reused software should be transparent to installers and include only the software modules actually being reused. During installation of a reused module, the installer should not be prompted for information that is not applicable to the new use for which the software is being applied. Additionally, the installer should be prompted to enter what is necessary to enter and not what was entered in the software's previous use.	Input that is required during configuration and installation of the IMA will be examined for extraneous input. The objective is met if all input is judged as relevant to the current use of the software. The objective is not met if the input refers to non-existent objects or purposes that are not part of the design of the current IMA.

INST-12 Manual input for configuration and installation shall be limited to responding to prompts and/or editing configuration file(s) and shall not involve entering information that the script can obtain automatically.

REQUIREMENT CLARIFICATION	TEST METHOD
The IMA administrator/installer should not be required to enter large amounts of data during the installation process. The installation process should prompt the administrator when input is required, but the amount of information should be kept small in order to lower the probability of input error. Entry of highly technical and product-specific data may	Configuration and installation of the IMA will verify the objective. The objective will not be met if, during the installation, low level commands and data need to be repeatedly entered from the configuration and installation documents.

increase the difficulty of determining where errors may have occurred during installation. The problem is particularly acute when the commands and data are beyond the knowledge level of the installer. The installation script should not prompt the installer for system or IMA information that can be obtained automatically. Examples of such information include hostname, addresses and operating system version.	

INST-13 The initial configuration and installation parameters shall be consistently set across the software components comprising the IMA.

REQUIREMENT CLARIFICATION	TEST METHOD
In some cases, inconsistently set parameters are due to a failure to reconcile the parameters between the various modules of the IMA software. This may happen, for example, when some modules of the IMA software are redesigned for a new release without examination of the other modules for resulting discrepancies or conflicts. The discrepancies or conflicts may exist in paths (including library paths) and environment variables, as set in various modules of the installation script.	Examine installation scripts and identify parameters (e.g., environment variables, path names, configuration settings) that are initialized more than once, even to the same value. The requirement is not met if the installer must manually set an installation or configuration parameter more than once (e.g., initializing the root directory for the application). The requirement is not met if the same installation parameter is not initialized with the same value in all cases and must be modified to enable the installation to continue normally.

INST-14 The IMA shall not reserve an explicit group identifier (ID) or user ID on Unix platforms or a specific user/group on NT platforms.

REQUIREMENT CLARIFICATION	TEST METHOD
Selection of user and group IDs across the DODIIS community can be difficult. An IMA cannot assume that any	The IMA configuration and installation guide will be examined for the presence or absence of instructions to add specific IDs for groups or users

given ID value or range of ID values is not already in use at a site where the IMA will be installed. Therefore, it is better to refer to logical user and group names instead of specific ID values. The IMA configuration and installation document may recommend one or more values for IDs, but if it does so, the documentation should also recognize the possibility of conflicts and include steps to resolve conflicts that do occur.	and users required by the IMA configuration. Verify that explicit default values are NOT required by executing the following commands: **NIS+:** *niscat passwd.org_dir* | *more* Continue by executing the command *niscat group.org.dir* | *more* **NIS:** *ypcat passwd* | *more* Continue by executing the command *ypcat group* | *more* **LOCAL:** *ls -l /etc/passwd* If the time indicates that the file has been modified during the installation, execute the command: *cat passwd* | *more* Continue by executing the command *ls -l /etc/group* If the time indicates that the file has been modified during the installation, execute the command: *cat group* | *more* **For NT:** Prior to installation of the IMA, execute the following steps: From the "Start" menu select: *Programs->Administrative Tools->User Manager* A list of local users will be displayed. Record the users listed. Following installation of the IMA, repeat the above sequence and examine

	the list of users in the User Manager. Make a note of any differences. Note: Adding users to the system requires that the user has administrative privileges. If the installation of the IMA was not done via a user with administrative privileges, then this step is unnecessary, and the requirement is met.

INST-15 The IMA shall not bundle Commercial Off-The-Shelf (COTS) or Government Off-The-Shelf (GOTS) software in its directory tree.

REQUIREMENT CLARIFICATION	TEST METHOD
COTS or GOTS software used by the IMA shall be installed as unbundled applications in accordance with the directory conventions specified in the DODIIS integration requirements. For example, if an IMA uses the COTS product *XYZmaker*, then the product shall be installed in the directory /opt/*XYZmaker*. There are no standard installation locations on the NT, although %SystemDrive%\Program Files\app is a defacto-standard. The IMA should default to the program files directory.	Following installation of the IMA, the directories containing IMA files will be examined. Review directories that might contain COTS or GOTS executables and data files by executing the command: Unix: *ls -latR* or NT: *dir ls* Verify that COTS or GOTS files are not bundled in with the IMA directory tree.

INST-16 Installation of the IMA shall not replace resources that are used by other IMAs.

REQUIREMENT CLARIFICATION	TEST METHOD
An IMA shall not replace or modify a resource such that it is configured solely for the preferences of that IMA and no other. This reasoning is applied to resources such as utilities,	Inspection of workstation resources will include files that are referenced during booting and initialization of the workstation. These files include inittab, ttytab, and inetd.conf, as well as resources that are referenced by operating system services and user applications during startup and execution, including as XKeysymDB, Xdefaults, and user preference files such as .cshrc.

environment declarations, and configuration files that may be used by more than one IMA. This includes not only the resources provided by the operating system, but also the resources that are provided by the DODIIS infrastructure. This requirement has broad uses. It applies to system-wide resources such as operating system functions like printing command shells and X11 resources, and it also applies to resources that are tailored for each user such as .Xdefaults files.	Appending IMA specific information to resource files is acceptable. Modifying objects that may be referenced by other applications is not acceptable.

INST-17 The IMA shall not overwrite or replace the native RPC map.

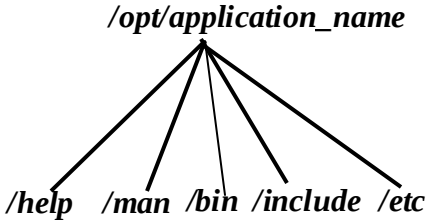
REQUIREMENT CLARIFICATION	TEST METHOD
Since an IMA cannot assume that it has control over the configuration of workstation resources, it cannot modify the default or standard RPC values. This may cause unpredictable behavior on the part of other applications. The IMA may append additional RPC values that do not conflict with registered RPC values.	**For UNIX**: Verify that the IMA design does not require overwriting or replacing the native RPC Map and that the installation of the IMA does not include overwriting or replacing the native RPC Map. The contents of the **/etc/rpc** file and the rpc map will be examined. **NIS+:** *ls -l /etc/rpc* If the time indicates that the file has been modified during the installation, execute the command: *cat /etc/rpc* Continue by executing the command: *cd /var/nis/data* or *cd /var/nis/<hostname>* *ls -l rpc.org_dir.log* If the time indicates that the file has been modified during the installation,

	execute the command: *niscat rpc.org_dir* **NIS:** *ls -l /etc/rpc* If the time indicates that the file has been modified during the installation, execute the command: *cat /etc/rpc* Continue by executing the command: *cd /var/yp/src* *ls -l rpc* If the time indicates that the file has been modified during the installation, execute the command: *ypcat rpc.bynumber* **LOCAL:** *ls -l /etc/rpc* If the time indicates that the file has been modified during the installation, execute the command: *cat /etc/rpc* **For NT:** Examine the RPC registry keys for modifications. Specific keys to examine are: HKEY_LOCAL_MACHINE\SOFTWARE\Description\Microsoft\Rpc HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Rpc HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\RPCLOCATOR HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_RPCSS HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RPCLOCATOR HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\RPCSS

INST-18 The IMA shall not require secure Network File System (NFS).

REQUIREMENT CLARIFICATION	TEST METHOD
There are documented incompatibilities between secure NFS and other NFS implementations.	The appropriate IMA documentation (e.g., Software Design Document (SDD), Configuration and Installation Guide) will be examined to verify that shared file IMAs do not require secure access. Verify that the "secure" option is not specified for any shared file IMA by executing the command: ***(SOLARIS): cd /etc/dfs*** For each file system in the file "dfstab" that is an NFS file system, verify that the "secure" option is not specified. Repeat this examination in the file "sharetab". This requirement is Not Applicable for the NT.

INST-19 IMA files shall be contained in **/opt/IMA_name** or /**opt/hostname#/IMA_name**.

REQUIREMENT CLARIFICATION	TEST METHOD
On UNIX systems, the IMA directory structure will be compliant with the following format:  As a result, an IMA that is exported to client workstations shall be located in ***/export/opt/hostname#/***	To verify the location of IMA files, execute the command: *find / -name application_name -print* where "application_name" is the name of the base directory containing IMA files or *cd /opt/application_name* *cd /opt/hostname#/IMA_name* *ls -latR*

application_name. The phrase "hostname#" simplifies distinguishing between network file IMA (NFS) servers and between disks on the same server by using the disk number (e.g., ***/export/opt/main_server1/amhs***). These conventions clarify the administration of exported IMAs and simplify the use of the automount function provided by Unix operating systems. This convention applies to all directories found under ***/opt***. For example, if IMA executables are located on a server, the executable path would be ***/export/opt/server_name/bin***, assuming that only one file system on the server is used for exported files.	Verify that the base directory is located either under /opt or /opt/hostname#, as appropriate. For IMAs that support Windows NT, the application folders should comply with the Microsoft Logo specification. For NT the application should be installed in "%SystemDrive%\Program Files\appname", where %SystemDrive% is the drive identifier where Windows NT is installed. The ability to override this directory should be provided.

INST-20 The IMA shall only use colors defined in the standard color data base.

REQUIREMENT CLARIFICATION	TEST METHOD
Referencing colors by logical names rather than hexadecimal strings improves the portability of the IMA. The standard color data base for X11 is defined in the file *rgb.txt* which is typically located in */usr/lib/X11*. The IMA should reference colors by the names included in this file since all systems that use the X11 windowing system will have the standard color data base. A IMA may not add new colors to the color data base.	Verify that the IMA does not redefine color names or numerical color codes. The platform color name data base file will be examined to determine if any changes have been introduced either after configuration and installation of the IMA or as a result of execution of the IMA by executing the command: SOLARIS: *ls -l /usr/lib/X11/rgb.txt* **or** *ls -l /usr/openwin/lib/rgb.txt* All IMA resource files (e.g., **.Xdefaults**, IMA files in **/usr/lib/X11/app-defaults**, etc.) will be examined for specification of colors by hexadecimal strings rather than by ASCII name that appears in the rgb.txt. It is acceptable to reference an existing color by its hexadecimal string. Such practice should be noted. It is not acceptable to reference a hexadecimal string that does not

	correspond to any color in rgb.txt. This requirement is Not Applicable for NT.

INST-21 The IMA shall use only fonts from the platform's native font set.

REQUIREMENT CLARIFICATION	TEST METHOD
The objective of this requirement is to reduce font problems when a window is exported from one platform to another. Unix vendors support the MIT X11 fonts almost universally. This requirement does not mean that the actual font encoding must be used. Instead, the fonts (by name) that are used by the IMA must be in the set distributed in X11R5. The actual font encodings are provided with the platform's X server. Windows NT supports a rich font set. In general, an IMA should not require a set of additional fonts. COTS applications that are integrated into the IMA may bring additional fonts with them. These fonts are considered outside the scope of this requirement.	Verify that the IMA uses the fonts that are provided in the platform's native font set. After the installation of the IMA, the directories that are touched during IMA configuration and installation will be examined to verify that the IMA does not include additional fonts. The IMA library directories should be checked. Directories, including IMA directories, should be examined for Motif and X11 libraries by executing the commands: *cd /usr/lib/X11* *ls -latR* *cd /usr/openwin/lib/X11* *ls -latR* Verify that the directories reviewed, including IMA directories, only contain. the fonts from the platform's native font set. Review each list, checking the modification times. A modification date during the IMA installation may indicate that the IMA is adding additional fonts to the IMA. Applications may include a font directory in the IMA tree. It may be necessary to examine the environment variables set by the IMA to determine in what directories the IMA searches for fonts.

INST-22 The IMA shall not require specific settings of permissions and ownership of browser files and directories.

REQUIREMENT CLARIFICATION	TEST METHOD
File and directory permissions and ownership must be set in	The permissions and ownerships of the browser files and directories will be

accordance with the site security policy. Default directory permissions after a browser installation enable users to do things such as download plug-ins as needed. This may violate the site security policy, and permissions must be set, after the browser is installed, to conform to the site security policy. The IMA design must take this and related file or directory configurations into account and be sufficiently robust in order to function properly with any adequate browser that has been installed and configured per site policy.	recorded before the IMA is installed. Following successful installation of the IMA the browser files and directories will again be examined to determine if any file or directory permissions or ownership has changed. If the IMA does not use a browser this requirement is Not Applicable..

INST-23 Installation of the IMA client shall not modify the home page settings of users.

REQUIREMENT CLARIFICATION	TEST METHOD
The IMA client should not require either manual or automated modification of home page settings for general users. A general user must be permitted to select his or her default home page. Some browsers support profiles that can specify settings such as default home page. By selecting the appropriate profile, the user can tailor his or her browser environment for the IMA without overriding the default settings. The IMA documentation can recommend definition of user profiles for this purpose.	Prior to installing and using the IMA, the user will start the browser and note the default home page. After the IMA has been installed and is ready for the general user, the user will start the browser and note the default home page. The default home page should be unchanged. If the IMA does not use a browser this requirement is Not Applicable..

INST-24 Installation of the IMA client shall not overwrite or modify default browser configuration settings of any user.

REQUIREMENT CLARIFICATION	TEST METHOD
Browser configuration settings are typically accomplished by	Prior to installing and using the IMA, the user will start the browser and note

each user rather than as global settings. The installation of the IMA client should not include an automated modification of any user's default browser configuration settings. Such changes may conflict with either the user's preferences or with site policy. Instead, the IMA documentation should provide sufficient information that each user can set his/her browser preferences or settings appropriately.	the default settings. After the IMA has been installed and is ready for the general user, the user will start the browser and note the default settings. The default settings should be unchanged. This procedure will be performed for each browser installed on the test workstation. If the IMA does not use a browser this requirement is Not Applicable..

INST-25 Installation of the IMA client shall not require modification of the user's mail and news configuration.

REQUIREMENT CLARIFICATION	TEST METHOD
The IMA implementation cannot assume that the mail and news activities of any user will be accomplished in a particular way. Browsers offer both mail and news functions but sites will vary as to the extent that these functions are used. The IMA cannot require the use of these features to implement some or all of its functions.	Prior to installing and using the IMA, the user will note the default mail and news configuration (i.e., which mail and news utilities are executed). After the IMA has been installed and is ready for the general user, the user will note the default mail and news configuration. The configuration should be unchanged. If the IMA does not use a browser this requirement is Not Applicable..

INST-26 The http server directory structure shall be separate from the html documents directory.

REQUIREMENT CLARIFICATION	TEST METHOD
The http configuration directory is typically separated from the Hyper Text Markup Language (html) documents directory in order to prevent web users from inspecting the server configuration files and discovering potential vulnerabilities.	Following installation of the IMA server, the http configuration will be examined to determine that the html documents directory is separate from the http server directory. e.g.:

	…/<*http server root directory*>/etc/httpd.conf ServerRoot "/opt/WWW/apache" …/< *html document root directory* >/etc/srm.conf DocumentRoot "/opt/WWW/htdocs" If the IMA does not use a browser this requirement is Not Applicable..

INST-27 An "index.html" or equivalent file shall be used to control default web pages.

REQUIREMENT CLARIFICATION	TEST METHOD
The use of a web interface to the IMA server should not permit a general user to browse through the server's directories and files. The existence of an "index.html" or equivalent file in the directory eliminates the ability of a user to obtain listings of directories and files on the web server. This file is specified in the server configuration. Without this file, if the URL for the web server specifies only a directory, then the httpd daemon returns a listing of that directory back to the user. If a file other than "index.html" is used, then this file should be specified in the documentation provided by the IMA. e.g.: …/apache/etc/srm.conf DirectoryIndex index.html index.cgi	Following the installation of the IMA server, the IMA documents directories will be examined to verify the existence of the "index.html" file in each directory under the Document Root directory. If the index.html file is not present, then the "srm.conf" file in the server configuration directory will be examined to verify that an index file is specified. The IMA directories will be examined to verify that this file exists in each directory under the Document Root directory. If the IMA does not use a browser this requirement is Not Applicable..

INST-28 All URLs referenced in html links shall contain at least one '.'.

REQUIREMENT CLARIFICATION	TEST METHOD
Depending upon its implementation/configuration, the browser may permit different settings for intranet (i.e., web sites within an organization's network) versus internet (i.e.,	The IMA will be executed through the browser. A representative set of web pages will be traversed and each URL will be noted. The expansion of each URL will be examined to verify that it contains at least one '.'.

web sites outside an organization's network). Settings for intranet web sites may be less restrictive than those for internet access (e.g., clients are allowed to execute JAVA applets from intranet sites but not from internet sites. The absence of a '.' in the logical host name usually indicates a site that is in the local domain or intranet and the browser will use appropriate settings. If a site is not part of the intranet and the referenced URL does not contain a '.', incorrect settings may be used by the client. A complete hostname in the URL will remove the ambiguity between intranet and internet access.	If the IMA does not use a browser this requirement is Not Applicable..

INST-29 The "httpd" and any IMA required daemons shall be started automatically when the server boots to multi-user mode.

REQUIREMENT CLARIFICATION	TEST METHOD
This is primarily a matter of level of effort on the part of the administrator to start the IMA web server/server. The automatic startup ensures that daemon are started with the same options each time and eliminates potential human error.	The system startup files for the server platform will be examined to verify that an entry for the daemon exists. The platform will be shut down and restarted. The daemons will start automatically without additional steps on the part of the test engineer.

INST-30 The web server shall log all connections and data requests that are received by the httpd daemon.

REQUIREMENT CLARIFICATION	TEST METHOD
Logging by the server assists in identifying operational problems as well as providing a record of access to the server. If logging is used as the primary auditing tool, then the log record should include the date and time, the host name, the files or services accessed, and, if possible, the	The IMA server configuration files will be examined to verify that logging by the httpd daemon is enabled. The test engineer will access the server through the browser interface. The test engineer will perform several test transactions with the IMA server. The

username.	test engineer will then examine the httpd log file and verify that the access is recorded and that the correct date, time, and host names are recorded. If the IMA does not use a browser this requirement is Not Applicable..

INST-31 The web server configuration shall implement Discretionary Access Control (DAC).

REQUIREMENT CLARIFICATION	TEST METHOD
Web servers provide the capability to configure and enable DAC to server resources. For example, the files access.conf enables access control on an httpd web server. The .htaccess defines access control per directory and can modify the global directives contained in access.conf.	After the IMA server has been installed, the web server configuration will be examined to verify that DAC has been enabled. For httpd servers, verify the presence of the "access.conf" file. The test engineer will access the server via a browser and evaluate the access control as defined in the access.conf file. The directories under the document root of the server document directory tree will be examined for the presence of .htaccess files. For directories that do not contain .htaccess files, the server will be accessed via a browser, and the test engineer will browse through each directory. The test engineer will evaluate whether he or she is able to exploit any security relevant functions due to the absence of .htaccess files. The requirement is met if the DAC configuration is defined and if the test engineer is unable to view information or exploit functions for which a general user is not authorized. If the IMA does not use a browser this requirement is Not Applicable.

INST-32 The httpd daemon shall be owned and run by a user name that is not superuser (Unix) or an administrative user (NT).

REQUIREMENT CLARIFICATION	TEST METHOD
Files directories and processes that are not directly related to operating system and platform management should not be	The ownership of the httpd executable file shall be examined to verify that it is not owned by root (Unix) or an administrative user (NT).

REQUIREMENT CLARIFICATION	TEST METHOD
owned by a superuser (root on Unix and an administrator users on NT) to limit security vulnerabilities and to avoid the need for superuser access to manage the IMA.	After the httpd has started, the ownership of the httpd process shall be inspected to verify that it is not owned by root (Unix) or an administrative user (NT). If the IMA does not use a browser this requirement is Not Applicable..

INST-33 Web IMA file names shall use appropriate file name extension for the content type.

REQUIREMENT CLARIFICATION	TEST METHOD
The standard file name extensions are used to improve portability of the IMA across platforms. The extension is used by a web browser to map the file to the appropriate application (e.g., viewer or plug-in) to view the file. Intelink documentation identifies the following common file extensions that are recognizable by web browsers. Note that this does not assume that the workstation has the needed applications installed; the IMA documentation should specify the viewers that are necessary for proper execution. File Type — Extension Plain text — .txt html document — .html, .htm GIF image — .gif TIFF image — .tiff XBM bitmap image — .xbm JPEG image — .jpg, .jpeg Postscript fil — .ps AIFF sound — .aiff AU sound — .au	The files in the web server documents directory will be listed using the command: *ls -latR* For each document file listed in the output, the file name extension will be matched to the Intelink standard file name extensions. The requirement is met if the file name extensions used by the IMA are included in the Intelink list of standard file name extensions. The requirement may also be met if file name extensions are not found on the Intelink list, but the file can be viewed by the commonly used web browsers (i.e., Netscape and Internet Explorer) without additional modification by the user beyond what is stated in the IMA documentation. If the IMA does not use a browser this requirement is Not Applicable..

QuickTime movie .mov MPEG movie .mpeg, .mpg This is not an all-inclusive list; browsers such as Netscape recognize a larger set of file name extensions, and this list can be modified by a user. The IMA documentation must include instructions to obtain, install, and configure needed viewers and plug-ins.	

INST-34 Readme files and errata sheets shall contain only last minute and errata type information that could not be incorporated into the final printing of the official configuration and installation guide.

REQUIREMENT CLARIFICATION	TEST METHOD
Readme files and errata sheets should not be used for whole portions of the configuration and installation document. Instead, these instructions should be in the formal configuration and installation guide. Typical use of readme files are for last minute and errata type information that could not be added to the deliverable guide before it was printed.	The contents of the readme files and errata sheets will be reviewed during the installation of the IMA. The objective is met when the configuration and installation is successfully completed using the configuration and installation document with minimal information, or no information, taken from readme files and errata sheets.

INST-35 The media delivered by the PMO to the JITF will include only the baseline for the release version under test.

REQUIREMENT CLARIFICATION	TEST METHOD
The PMO will deliver to the JITF software that reflects the delivery to DODIIS sites. This should only be the baseline release version that is cleaned of underlying development environment files. Old development data files, scripts, backups, and other extraneous files that have no place in the baseline should not be distributed. This also applies to development data files, scripts, backups, database files, etc.,	The directory tree of the delivered media and the installation application will be examined for files and directories that are extraneous to the software baseline.

that are planned for future releases.	

INST-36 The installation and configuration of the IMA shall be completed in 20 working hours.

REQUIREMENT CLARIFICATION	TEST METHOD
Installation and configuration covers the entire processing of loading software and modifying configuration files and parameters for successful operation of the IMA. It does not include loading of IMA data. The 20 hour limit is 20 sequential hours. If the installation is permitted to execute overnight (e.g., to extract software from media), the overnight hours are included in the time required to install the IMA.	The date and time at the beginning of the installation will be recorded. Once the IMA has been installed and configured, the date and time will again be recorded. Installation is completed after all required steps in the installation and configuration guide are performed successfully AND software verification is performed successfully. The time required to execute the software verification steps is not included in the time to install the IMA.

INST-37 The IMA design shall not prohibit installation and operation of the application on a platform shared by other applications.

REQUIREMENT CLARIFICATION	TEST METHOD
One goal of the DODIIS architecture is to give the sites flexibility in selecting how each IMA will be installed and used. An IMA that, by design, permits sharing of a platform with other IMA servers allows sites to select platforms based upon IMA performance and resource usage. An IMA that, by design, requires a dedicated platform may hinder integration of the IMA into a site simply because computing resources - i.e., platforms and software - are duplicated unnecessarily. Resource sharing by applications should include more than simply coexisting on the same platform. It should include sharing computing resources such as data servers. At this	Application configuration and installation guide will be inspected to verify that the ability to share a server platform is specified. During installation and configuration of the IMA, the test engineers will note the configuration parameters that will prevent the IMA to operate on a platform shared with other applications.

time, guidelines and conventions to accomplish this are not specified. These guidelines and conventions must be documented to allow IMAs to fully share computing resources efficiently.	

3.3 ENVIRONMENT

ENV-1 The IMA shall not modify system files in any way that causes the computing platform to fail to boot if the IMA client or IMA server is unavailable.

REQUIREMENT CLARIFICATION	TEST METHOD
An IMA cannot assume that it "owns" the platform or platform resources. The workstation or server is a user tool, and accessing a specific IMA is only part of what a user may do during a login session. Since all IMAs at the site are integrated into the operating environment, the inaccessibility of a particular IMA does not mean that the user will not be able to perform useful work. The actual booting of the workstation must not be dependent upon the accessibility of any or all IMA servers. Likewise, a server platform may host one or more server IMAs. Even on a server platform, the booting process must not be modified to halt or in some way hinder the boot process if the server IMA is unavailable for some reason.	The IMA configuration and installation guide, will be reviewed to determine if any boot files are modified by the installation. The documentation will be also be examined to determine what workstation resource files are modified by the installation. Following installation of the IMA, the boot files of the workstation will be examined to determine if the modifications made by the IMA installation process will prevent booting if the IMA server is unavailable. The files examined will include the init files for the operating system: (e.g., for Unix) */etc/rc** */sbin/rc** */etc/services* */etc/*.conf* On the NT, init files for the OS include: Config.sys, Autoexec.bat, IO.SYS, MSDOS.SYS, WIN.INI, and SYSTEM.INI. The registry also plays an important role in the boot process. The NT Analyzer will be used to identify changes to these files. After successful configuration and installation of the IMA, on both a server platform and on general user workstations, perform the following: Halt a general user workstation. Halt the host on which the IMA server executes. After the server host has halted, reboot the user workstation. The workstation will complete its boot sequence and the XDM login screen will

	be displayed.

ENV-2 Execution of the IMA shall not replace or alter system resources that are used by other IMAs.

REQUIREMENT CLARIFICATION	TEST METHOD
An IMA shall not replace or modify a resource such that it is configured solely for the preferences of that IMA and no other. This requirement applies to workstation resources such as utilities, environment declarations, and configuration files that may be used by more than one IMA. This includes not only the resources provided by the operating system, but also the resources that are provided by the DODIIS infrastructure. Operating system and infrastructure patches are also covered by this requirement; the IMA cannot back out a patch and replace it with a newer version. The requirement applies to system-wide resources such as operating system functions like printing command shells and X11 resources and to resources that are tailored for each user such as .Xdefaults files.	On Solaris platforms, the process monitor will be used to identify files that are opened for writing by the IMA. For each file that is a system or user resource, the test engineer will verify that the IMA does not overwrite the file or replace any information in the file that is not specific to the IMA. On the NT, output from the Analyzer tool will be examined. The test engineer will verify that patches have not been backed out during the IMA installation.

ENV-3 The IMA shall not prevent or alter login if the IMA server or client is unavailable.

REQUIREMENT CLARIFICATION	TEST METHOD
Stopping the execution of the IMA server software, halting the host on which the IMA server executes, or modifying the client IMA configuration so that the IMA client software is unavailable will not affect the user's ability to login to the	After successful configuration and installation of the IMA on both a server platform and on general user workstations, perform the following: Stop the execution of the IMA server software. The operating system and

workstation.	other services of the host on which the IMA server executes will still be available. After the IMA server has stopped, ping the host to verify that it is running and accessible. Login to a general user workstation. The login will complete normally and the user will be presented with the session environment and desktop, if one is configured for that session. Halt the host on which the IMA server executes. After the host has halted login to a general user workstation. The login will complete normally, and the user is presented with the session environment and desktop if one is configured for that session. Restart the server host and the IMA server software. On a general user workstation, modify the client IMA configuration so that the IMA client software is unavailable. This can be done by either a) moving the client executable file(s) to an inaccessible location on the user workstation or b) temporarily renaming the client executable file(s). If the client server is obtained via file sharing from an IMA server, either a) or b) must be done on the IMA server. Access to the IMA server is not altered. Once this has been completed, log out of the workstation. Login to the general user workstation as a general user. The login will complete normally, and the user is presented with the session environment and desktop, if one is configured for that session.

ENV-4 The client application(s) of the IMA shall launch from the background menu or from an icon on the desktop.

REQUIREMENT CLARIFICATION	TEST METHOD
This objective verifies that the client appl.ications for the IMA will launch successfully from the background menu selection or by initializing the IMA from an icon on the DODIIS desktop.	The requirement is not met if the application must be started by the user from a command line. Following configuration and installation of the IMA on the general user

	workstation, the background menu item(s)/icon corresponding to the IMA will be selected. Selected test cases from the IMA test plan will be executed if normal operation of the IMA is not readily apparent.

ENV-5 The server application(s) of the IMA shall not require manual launching by an administrator.

REQUIREMENT CLARIFICATION	TEST METHOD
Server applications should start automatically in order to be available to requests from users at all times when the server platform is operating. A server application can be started at the time the platform boots (e.g., by execution of a boot script during system booting). It can also be spawned by a system process (e.g., "inet.d") whenever a user request is received. The administrator should not be required to manually start the server application for normal operation.	The requirement is not met if server applications for the IMA must be started manually. If the IMA design implements restart of the server applications for the IMA during system reboot, the server platform will be halted and rebooted. Following the completion of the reboot, the process table will be examined. The requirement is met if the server processes for the IMA are executing. If the IMA server applications are spawned by a system process upon receipt of a user request, the server platform will be set in an idle state (i..e., no user requests are being processed or are pending). The process table will be examined to verify that no server applications for the IMA are executing. A request for data will be transmitted from a client application for the IMA. The process table for the server platform will be examined again to verify that IMA server applications are now running.

ENV-6 IMA environment variables shall be defined in the form of PRODUCT_VARNAME.

REQUIREMENT CLARIFICATION	TEST METHOD
For UNIX systems, developers should assume that the following variables are global and have been defined by the site: *PATH, HOME, TERM, TZ, LOGNAME, SHELL*, and *TMPDIR*. The developer shall only define variables that are	The IMA configuration and installation guide will be examined to verify that environment variables initialized by the IMA are defined in the form of PRODUCT_VARNAME.

specific to the IMA and follow the format specified in this requirement. By following the variable naming convention, the probability that the IMA may overwrite or redefine variables of other IMAs is limited. Note that variables that are defined locally to the execution of the IMA (e.g., from a launch script) will not conflict with variables that are defined either globally or locally by other IMAs. Local definition of variables is preferred to globally defining variables that have meaning only to one IMA. For NT, there are several environment variables reserved: ComSpec, LOGONSERVER, HOME_DRIVE, HOME_PATH, NUMBER_OF_PROCESSORS, OS, PATH, PATHEXT, PROCESSOR_ARCHITECTURE, PROCESSOR_LEVEL, PROCESSOR_REVISION, SYSTEM_DRIVE, SYSTEM_ROOT, TEMP, TMP, USERDOMAIN, USERNAME, USERPROFILE, windir NOTE: If PATH references the environment variable %SystemRoot%, the environment variable must appear first. If %SystemRoot% is not used to refer to the Windows NT Directory in the Path Statement, then the order of the path statement does not matter. For example, if the PATH is set to "%SystemRoot%;C:\", it must appear in that order – it cannot be "C:\;%SystemRoot%". However, if PATH is set to "C:\WINDOWS_NT;C:\", then the order does not matter, since the environment variable does not have to be resolved.	Following configuration and installation of the IMA, the launch scripts used to invoke execution of the IMA will be examined to verify that all environment variables initialized in the launch scripts also follow the required format. The examination will include any data added to the infrastructure session management configuration files during the configuration and installation of the IMA.

ENV-7 The IMA shall use the directory defined by the TMPDIR environment variable for all temporary files.

REQUIREMENT CLARIFICATION	TEST METHOD
On Unix systems, TMPDIR is a globally defined environment variable that is initialized at the beginning of any login session in the DODIIS infrastructure. TMPDIR defines a directory that is used for temporary files. Temporary files are files that have no use or meaning after the application has terminated. On Unix systems, TMPDIR typically points to /tmp which is automatically cleared when the workstation reboots. Conversely, the directory defined by TMPDIR should not be used for any files that might have use beyond the user's session. The IMA has no control over when the temporary directory will be cleaned, and such files could be lost without any notification.	Following the installation of the IMA, the IMA launch script installed via the infrastructure Session Management Utility will be examined to verify that TMPDIR is not redefined and that an additional environment variable defining temporary file space is not initialized. On NT, the environment variables TMP or TEMP are used to identify the location of temporary files. Verify that the IMA uses the directory defined by the TMPDIR environment variable for all temporary files.

3.4 OPERATION

OPS-1 IMA file names shall consist of valid characters for file names and shall be restricted to the maximum length of 128 chars for UNIX/Solaris systems and 255 characters for Windows NT systems.

REQUIREMENT CLARIFICATION	TEST METHOD
This requirement is a general requirement for all files stored on a workstation or server. Valid characters for UNIX/Solaris are defined in the X/OPEN XPG4 recommended character set, and in the Microsoft Logo specifications for Windows NT. Valid characters are 0-9, Aa-Zz, . (dot) + (plus), - (minus), : (colon) and _ (underscore). Other characters are invalid because they may have meaning as meta characters, have meaning to the shell, or be difficult to reproduce (i.e., hidden characters).	To verify the files created do not exceed the 128 character limit, execute the command: *ls -latR* View the output of this comment and verify the structure and length of each file or directory name. This procedure must be done for each directory touched by the IMA installation.

OPS-2 The IMA shall use the platform's native keyboard map.

REQUIREMENT CLARIFICATION	TEST METHOD
On Unix platforms, the keyboard, including the mouse buttons, is owned by the X server, but it is a shared resource. Keyboard mapping refers to the mapping of the physical keys, which are identified by "keycodes", to events passed by the Xserver to a client application. The events are described by "keysyms". Each keycode is mapped to one or more keysyms. The actual keysym (interpretation of the pressed key) depends upon the actions of modifier keys (Shift, Caps_Lock, etc). The list of keysyms associated	Typically, keyboard map modification is done in an application launch script via the "xmodmap" utility. To evaluate this requirement, execute the command: *cd /<scripts directory>* *grep xmodmap ** If this command finds any xmodmap commands in the IMA's scripts, the IMA is likely modifying the keyboard map. This can be determined by the options passed to the xmodmap command. The -e option is used to change either a keysym listing or a mapping of keysyms to a keycode.

with a specific keycode can be changed by any application. Since the keyboard is a shared resource, any changes made by one client application are global to all applications. Therefore, problems can occur when individual IMAs remap the keyboard for their own purposes. A subtler issue is the definition of keysyms, since these values determine the actions of the mouse and the appearance of characters in a client window. keysyms are defined in /usr/lib/X11/XKeysymDB (or /usr/openwin/lib/X11/XKeysymDB). The infrastructure provides a default XKeysymDB file. Altering this file does not change the keyboard map. IMAs may append (but not overwrite) to this file or may actually refer to a different XKeysymDB file, providing that this reference is not global to all applications. Most IMAs will have no need to use anything but the default XKeysymDB file. Under NT, there is no file map file. File map information is maintained in the NT registry. However, it is possible for an application to modify the native mapping of characters for the specific application. There are no files to examine to ensure that this is not done.	Alternatively, the xmodmap command can be used to capture the current keyboard map. Prior to starting the IMA, execute the following commands: *xmodmap -pm >/tmp/mod.map* (modifier map) *xmodmap -pk >/tmp/key.map* (keyboard map) *xmodmap -pp >/tmp/pointer.map* (pointer or mouse map) After starting the IMA, repeat the three commands in a separate command window and save the output to three different files (e.g., mod1.map, key1.map, pointer1.map). Compare the contents of the pairs of maps by either inspection or via the "diff" command. If the IMA has not changed any of the maps, then there will be no differences. The IMA may append keysym entries to the default XKeysymDB file. Compare the XKeysymDB file prior to IMA installation to the file after the IMA has been installed. The requirement is not met if any keysym entries have been overwritten. The IMA may install and use a different XKeysymDB file than the one found in ***/usr/lib/X11***. The IMA must set the environment variable XKEYSYMDB to the path of this alternate file. This variable must be set locally; the requirement is not met if the variable is set globally. The variable is set globally if it is initialized at the time of user login. To determine if the variable has been set globally do the following: On the command line before starting the installation enter: *echo $XKEYSYMDB* Verify that the variable has no value.

OPS-3 The execution environment that exists at the time of IMA launch shall not conflict with either the user's overall operating environment or the execution environment of other applications.

REQUIREMENT CLARIFICATION	TEST METHOD
The execution environment of the IMA is defined by the environment variables set by the operating system, the infrastructure, and the IMA. The execution environment should not result in ambiguous or incorrect references to commands or files due to assumptions by the application with regard to environment settings. Additional areas of conflict in the execution environment include keyboard mapping, use and modification of files shared with other IMAs operating system configuration files, and use and modification of root window resources.	Evaluation of this objective is accomplished by: 1. Evaluating the integration of the IMA into the infrastructure sessions and the associated definition of global variables, noting the search path variables, such as PATH and LD_LIBRARY_PATH; 2. Identifying operating system configuration files that are modified during IMA installation and configuration. 3. Reviewing the launch scripts for definition of global variables and reference/modification of shared resource files. 4. Identifying changes, if any, to the keyboard map and root window resources. 5. Evaluating changes (if any) in the IMA's processing parameters.

OPS-4 The IMA shall not contain configuration files or tables that duplicate information already contained in the operating system configuration files.

REQUIREMENT CLARIFICATION	TEST METHOD
The IMA design should not include duplicate information that is already contained in and distributed by the DODIIS infrastructure. This includes information that is available from an operating system service such as NIS/NIS+ and information that is maintained by other infrastructure services such as Domain Name Service. Duplication of this type increases the risk of losing synchronization with other IMAs that are utilizing the same information. For example, placing	The IMA design documentation and configuration and installation guide will be inspected to determine if any redundant information is being maintained by the IMA. After the IMA has been installed, the configuration files created or modified by the IMA will be inspected for inclusion of redundant information. Redundant information will include, for example, host name/IP address pairs, reserved port numbers (except for the IMA itself), and the local host name.

the name and IP address of the IMA server in an IMA configuration file can affect the execution of the IMA. An update to the IMA configuration file would also be required if the IP address is changed by the system administrator.. Unless the IMA administrator has kept detailed configuration records, he/she may not be aware that this must be done until the IMA fails to execute properly.	

OPS-5 The IMA shall not use extensions to the Window System (X or Windows NT) that are not supported by the infrastructure.

REQUIREMENT CLARIFICATION	TEST METHOD
X Window System extensions improve the ability of the workstation to display graphics such as post script or animation. In order for IMAs to operate on any DODIIS platform that uses the X Window System, the IMA must implement and comply with a common set of extensions. The X Consortium defines a set of extensions to the X Window System. In order for an application to use any extension in this set, the X server must support the extension, and the necessary library must be present on the platform that is executing the IMA. The X server provided by the Solaris operating system supports the following X extensions: - Display Post Script (DPS) - X Input Extension - Double Buffer Extension - Shape Extension - Shared Memory Extension - Miscellaneous Extension	If the IMA uses extensions to the window system that are not supported by the infrastructure X server, it must either place additional libraries in the standard system directories, such as **/usr/openwin/lib** or modify the library search path via the environment variable LD_LIBRARY_PATH. In addition, the X server must be modified or replaced to support the additional extensions. After installation of the IMA, the directories that are touched during IMA configuration and installation will be examined to verify that the IMA does not include or bundle additional libraries for the window system extensions. The installation must not overwrite any operating system libraries. The native X server will be checked to verify that it has not been replaced during installation of the IMA. If the IMA installation includes loading of an X server, the documentation will be examined to determine if the execution of the IMA requires using this X server in place of the native X server. The requirement is not met if the IMA adds additional X extension libraries to the platform during installation, overwrites the native X extension libraries, or

- XC-MISC - X Imaging Extension The extensions require the libraries "libXext", "libXi", and "libdps*" in /usr/lib/X11 (/usr/openwin/lib/X11). These libraries are part of the infrastructure, and the IMA does not need to add them during installation.	if an additional X server is loaded on the platform during IMA installation and is required for execution of the application. This requirement is Not Applicable for NT.

OPS-6 The IMA shall use the infrastructure print utility for printing hard copy.

REQUIREMENT CLARIFICATION	TEST METHOD
This requirement is applicable for both IMA client and IMA server processes and requires that destination printers are managed by the infrastructure print management utility.	This requirement is met by verifying that the infrastructure print management utility is used to manage the destination printer and by inspecting hard copy printouts.

OPS-7 Administration of the IMA shall not require access to privileged user accounts.

REQUIREMENT CLARIFICATION	TEST METHOD
Once the IMA is installed and configured, administrative functions that specifically address access to and operation of the IMA should not require logging in as root or as an administrator. This approach reduces the probability that administrative changes for one IMA may affect the operation of other IMAs or the operation of the workstation or server platform itself. Access to IMA administration functions can be implemented in one of several ways: 1. A functional user ID can be used. This ID is placed in a restricted Unix group for IMA administrative	After the IMA has been installed, executable files that provide administrative functions will be identified. The permissions on each file will be examined to verify that the IMA administrator does not require superuser (root on Unix and administrator on Windows NT) privileges to manage the IMA.

functions. In this approach, the administration functions are typically available through menu selections in an IMA window. 2. The user ID that is used for IMA administration is a separate user ID that reflects the greater privilege and trust required for IMA administration. 3. The IMA administration functions are accessible by user IDs that are associated with administration of site software. The use of an infrastructure trusted role is appropriate in this approach. The IMA design may require a combination of the approaches listed above. For example, an IMA may provide administrative functions from its main window to certain user IDs and also require access to a privilege user ID for data base administration.	

OPS-8 The administrator shall be provided with utilities and tools to add, modify, or delete IMA users.

REQUIREMENT CLARIFICATION	TEST METHOD
This objective refers only to managing users of the IMA, not to the definition and management of workstation users (i.e., Unix or NT accounts). The latter is performed via the infrastructure user management tool. Many IMAs will not provide or need any tools other than infrastructure User Management. User management should be limited to doing what is needed to give the user access (or take away access) to the IMA and its data. If access can be achieved by using the already existing tools of the infrastructure, then no additional utilities are required. In the case of IMAs that	The IMA administration documentation will be reviewed to identify the approach to IMA user management. The tools to add, modify, or delete IMA users will be identified. After the IMA has been installed, the identified tools will be located. The tools will be evaluated to determine if any of the tools is a redundant implementation of an operating service or infrastructure, including data base management, service, etc. This requirement is Not Applicable if the IMA does not provide and does not require additional tools to manage IMA users.

rely on data bases, the management tools of the data base management IMA are sufficient, and the IMA does not have to provide additional, redundant tools.	

OPS-9 The IMA shall use infrastructure management utilities to manage and distribute IMA, user, and security data.

REQUIREMENT CLARIFICATION	TEST METHOD
The IMA developer must use the management services of the DODIIS infrastructure wherever it is appropriate. Since the trend in DODIIS is toward shrink-wrapped IMAs, there should be, in general, few requirements for an IMA to manage system resources such as user data and security data. Management requirements for the IMA must pertain solely to areas of management that are specific to the IMA rather than to areas of management that pertain to the system in general.	The appropriate IMA documentation (e.g., SDD, Trusted Facilities User's Guide (TFUG)) will be examined to verify that application, user, and security management are performed with infrastructure management utilities. The administration tools provided by the IMA will be identified. After the IMA has been installed, the administration tools will be exercised to evaluate their functions. Executing the tools will verify that the IMA utilities do not duplicate infrastructure tools to manage and distribute application, user, and security data.

OPS-10 IMA files that "grow" as a result of IMA execution shall not fill or result in exhausted file system space.

REQUIREMENT CLARIFICATION	TEST METHOD
Many IMAs use files that are continually increasing in size. Such files are log files, temporary files, and audit files. If the IMA relies on the syslog file, temporary directory, and audit directories provided by the infrastructure, then managing these growing files becomes the system administrator's responsibility and is no longer the responsibility of the IMA. However, if the IMA places its logs, temporary files, and/or audit data in other locations, then the IMA documentation should clearly identify these locations. Additionally, the IMA	During execution of the IMA, the IMA process will be monitored via the "truss" process to identify files that are opened for writing by the IMA. For each such file identified, the test engineer will evaluate if the file has the potential to exhaust file system space. If this condition is met, the test engineer will verify that each file is managed to avoid exhausting file system space (e.g., deletion or compression of the temporary files). If the IMA uses a DBMS, then the IMA administrator must be aware that the transaction logs must be managed.

design should account for these growing files and provide the means to automatically reduce them as needed. Data base Management System (DBMS) transaction logs are also covered by this requirement. If the IMA implements a transaction log within the DBMS, then the IMA administration documentation must provide guidelines to ensure that the log does not exhaust space within the DBMS and stop the DBMS. This is particularly critical if the IMA is one of several applications sharing a data server; the transaction log associated with the IMA could crash the data server, thus causing disruption of service to other IMAs.	The IMA administration documentation will be examined to verify that guidance for managing the transaction log is provided.

OPS-11 The loss of connectivity between the IMA client process and the IMA server process shall not affect the behavior or operation of other client workstation applications or utilities.

REQUIREMENT CLARIFICATION	TEST METHOD
Connectivity refers to the ability to pass protocol data units (e.g., packets, TCP/IP transmission units) between the IMA client process on the user's workstation and the IMA server process executing on either the same workstation or on another platform. From the perspective of the user, connectivity can be lost if the server process is terminated unexpectedly or if the network path between the two processes is broken in some way. The loss of connectivity should not cause other processes on the workstation, including the operating system, to operate incorrectly, such as hanging or terminating unexpectedly. The IMA itself may hang or terminate depending upon the IMA design. For browser-based applications, the browser itself may hang. It	The objective will be verified in two ways: 1. The IMA server process will be terminated during an IMA client session with the server without normal notification to the client. The operation of the user's workstation will be evaluated to determine that no process, other than the IMA client process itself are affected. 2. The network connection between the IMA server process and the IMA client process will be broken during a client session. This can be efficiently accomplished by disabling the network interface of the platform on which the server process is executing. This does not affect the operation of the network itself. The operation of the user's workstation will be evaluated to determine that no process other than the IMA client process itself is affected.

is acceptable that the web access/transfer can be stopped or the window closed. In some cases, the browser may have to be terminated; this is outside the scope of this requirement.	

OPS-12 Disorderly termination of the IMA shall not affect the execution or behavior of other applications.

REQUIREMENT CLARIFICATION	TEST METHOD
The activity of the IMA should not affect the activity of other applications executing on the same platform or in the same operating environment (i.e., the DODIIS site). Disorderly termination can occur if the IMA exits due to a software error or invalid user action or if the IMA is unexpectedly halted by a user or administrator action. Other applications should continue to operate normally when such events occur.	This objective will be verified in the following manner: 1. The IMA will be started in a typical user session. At various points in the session (e.g., initial startup, data transfer/review, query/response), the client IMA will be terminated by using the "kill" command from a shell window. For web-based applications, the browser is considered the client IMA. 2. The IMA will be started in a typical user session. At various points in the session (e.g., initial startup, data transfer/review, query/response), the user will log out of the workstation without first exiting the IMA. In both cases, the operation of the user's workstation will be evaluated to determine that no other processes are affected. In order to test the effect of disorderly termination of the IMA server processes, the following steps should be followed for servers that are using the DBMS. # cd …/sybase/bin/isql -Usa -P<sa password> 1>shutdown SYB_BACKUP (To shutdown the backup server) 2> go 1> shutdown (Shuts down the main data server) 2> go # sync # sync

	# halt If the data server is shared among several applications, then these applications will be affect by these steps. Verify that applications and operating system services running on the same platform as the data server are still running properly. Restart the data server. Terminate the IMA server processes. Verify that the applications and operating system services running on the same platform as the data server are still running properly. This requirement is Not Applicable for NT.

OPS-13 Disorderly termination of the IMA shall not result in incorrect behavior of the IMA when the IMA is restarted.

REQUIREMENT CLARIFICATION	TEST METHOD
Disorderly termination can occur if the IMA exits due to a software error, invalid user action, or if the IMA is unexpectedly halted by a user or administrator action. The IMA itself should recover from the disorderly termination and execute properly when restarted. This may be difficult to achieve for IMA server processes, such as data base servers. The IMA design should plan for the likely occurrence of disorderly termination so that recovery will be possible.	This objective will be verified in the following manner: 1. The IMA will be started in a typical user session. At various points in the session (e.g., initial startup, data transfer/review, query/response), the client IMA will be terminated by using the "kill" command from a shell window. 2. The IMA will be started in a typical user session. At various points in the session (e.g., initial startup, data transfer/review, query/response), the user will log out of the workstation without first exiting the IMA. 3. The IMA server application will be started. While users are accessing the server via client IMA applications, the server will be shut down. For an application that uses a DBMS, the database server will be shut down via ISQL first in order to avoid corruption of the database. The steps outlined in OPS-12 will be used.

	Following each case, the IMA will be restarted, and the normal operation of the IMA will be verified**.** This requirement is Not Applicable for NT.

OPS-14 Orderly termination of the IMA shall not affect the execution or behavior of other applications.

REQUIREMENT CLARIFICATION	TEST METHOD
If the normal process of starting and stopping the IMA affects the operation of other processes on the workstation or of the IMA itself when it is invoked again, the IMA design is unsatisfactory. Sample test scenarios will be performed in which the IMA is started, used in typical manner, and then terminated by the recommended steps.	This objective will be verified in the following manner: The IMA will be started in a typical user session. At various points in the session (e.g., initial startup, data transfer, query/response), the client IMA will be terminated by using the "exit" command or button from the IMA main window. The IMA server application will be started. While users are accessing the server via client IMA applications, the server will be shut down using the IMA documented steps for stopping the server. Following each scenario, the operation of the user's workstation will be evaluated to determine that no other processes are affected.

OPS-15 Disorderly shutdown of the client workstation while the IMA is executing shall not affect the behavior or operation of the IMA on other workstations.

REQUIREMENT CLARIFICATION	TEST METHOD
There should be no effects that are attributable to the IMA on other workstations if the user's workstation is shut down while the IMA is active. Once the workstation or server platform is rebooted and the IMA is restarted, the IMA should execute normally.	The IMA will be started on the user's workstation. Once the IMA is active, the workstation will be shut down (i.e., halted). The IMA processes on other workstations in the test environment will be evaluated for normal operation.

OPS-16 Disorderly shutdown of the client workstation while the IMA is executing shall not result in incorrect behavior of the IMA when the IMA is restarted.

REQUIREMENT CLARIFICATION	TEST METHOD
There should be no effect on other workstations that are attributable to the IMA if the user's workstation is shut down while the IMA is active. Once the workstation or server platform is rebooted and the IMA is restarted, the IMA should execute normally.	The IMA will be started on the user's workstation. Once the IMA is active, the workstation will be shut down (i.e., halted). After the workstation is rebooted, the IMA is restarted, and the normal operation of the IMA will be verified.

OPS-17 User log out of the client workstation while the IMA is executing shall not affect the behavior of the IMA or the behavior of other applications in the user's next login session.

REQUIREMENT CLARIFICATION	TEST METHOD
Once the user logs in to the workstation and invokes the IMA, the IMA should execute normally. The IMA may not execute normally if the user log out and consequent termination of the IMA leaves a residue of lock files and similar objects that will affect the behavior of the IMA. There should be no effect on other applications that are started in the user's next login session	Test scenarios will be run in which the IMA is started and the user logs out at various points in the scenario. After the user logs back into the workstation, the operation of other applications in the login session should not be affected. The next scenario will be started, and the normal operation of the IMA will be verified. Following the verification, the user will log out of the workstation at a different point in the scenario. . It is not acceptable that the IMA that was running on the workstation remain active once the user logs out.

OPS-18 The IMA shall exhibit consistent behavior across all supported operating systems and platforms.

REQUIREMENT CLARIFICATION	TEST METHOD
The IMA design should enforce a uniform look and feel across all of the platforms and operating systems supported by the IMA. Limitations due to the hardware and operating system that prevent a uniform look and feel should be identified in the IMA design documentation. There should be no differences in the functions provided by the IMA to the user regardless of the platform and operating system.	Ad hoc testing will be performed on each platform in the test environment that is supported by the IMA. A combination of testing and inspection will be used to verify that there are no differences in the IMA function regardless of the platform and operating system.

OPS-19 The IMA shall not duplicate functions provided by support applications.

REQUIREMENT CLARIFICATION	TEST METHOD
A primary objective of establishing a common infrastructure and common support applications for DODIIS sites is to eliminate the redundant implementations of functions by IMAs. An IMA must only implement functions that are specific to its scope. Otherwise, it must use the services provided by the infrastructure support applications.	The IMA configuration and installation guide will be examined to verify that the IMA does not include functions that are provided by DODIIS support services. This will include services provided by the infrastructure, System Acquisition Support Service (SASS) applications, and operating system utilities. After installation of the IMA, the IMA directories will be examined for modules that duplicate support services. Verify that the IMA is not duplicating functions provided by support applications. Examine the IMA directory tree and execute the command: Unix: *ls -latR* NT: *dir ls* Examine appropriate directories to determine if duplicate support services are being used.

OPS-20 The IMA shall use shared libraries for UNIX/Solaris and DLL's for Windows NT.

REQUIREMENT CLARIFICATION	TEST METHOD
Use of shared libraries if supported by the operating system results in less disk space required to store the IMA.	Determine if shared libraries are used by IMA software. Following installation of the IMA, the IMA binary files will be examined using the "file" utility to determine if dynamic linking of libraries is employed. For UNIX: To verify which IMA binaries use shared libraries execute the command: *file <binary name>* If libraries are dynamically linked execute the command:

	(SOLARIS) ldd <binary name> to determine which libraries are linked to the IMA. For NT: From the command prompt execute: *CheckDLL* The CheckDLL program is a batch file that will scan Executable and library files located in a directory looking for references to Dynamic Link Libraries. Note that if an executable does not reference a DLL, it does not mean the IMA failed the requirement. It is necessary to consider what the function of the application is and if it is possible to utilize a DLL. IMAs that have installable options typically store the code for the option in a DLL.

OPS-21 The IMA shall not require use of a browser with acceptance of cookies enabled.

REQUIREMENT CLARIFICATION	TEST METHOD
Many browser-based applications rely on cookies written by the web server and stored locally by the browser. This practice has been widely accepted and, at the current time, no security vulnerabilities relating to the use of cookies have been identified. However, site security policy may require acceptance of cookies to be disabled and the IMA must be able to function properly with this restriction.	The browser will be configured to refuse cookies by doing the following: On the browser menu bar: Select *Edit* Using the pull down menu select *Preferences* Click *Advanced* to display the Cookie Options box Make necessary adjustments. The IMA will then be accessed. The behavior of the IMA will be evaluated to verify that it is functioning normally. This requirement is Not Applicable if the IMA does not use a browser.

OPS-22 Web pages shall not contain animations and animated GIF files that do not implement mission functions.

REQUIREMENT CLARIFICATION	TEST METHOD
System resources that are required to display animation may cause additional delays in downloading the objects that implement animation or may cause performance problems for the IMA or for other IMAs. Animations must be limited to those which are clearly necessary to accomplish one or more mission functions.	The execution of the IMA will be inspected to verify that animations and animated GIF files have functions pertinent to the scope of the IMA. If the IMA does not use a browser this requirement is Not Applicable

OPS-23 Web pages shall not contain elements that obscure or interfere with reading clarity.

REQUIREMENT CLARIFICATION	TEST METHOD
This requirement emphasizes that IMA web pages should focus on mission functions rather than artistic additions that may distract from the IMA mission.	The execution of the IMA will be inspected to verify that IMA web pages do not contain over busy background patterns, low contrast between foreground and background, non-functional blinking text, or other elements that would impact reading clarity. Blinking text may be used to implement or enhance mission functions (e.g., a flashing security alert). This requirement is Not Applicable if the IMA does not use a browser.

OPS-24 Large graphic images shall be downloaded on demand. A small icon of the image shall be displayed on the web page and linked directly to the full-sized image.

REQUIREMENT CLARIFICATION	TEST METHOD
Large graphic images may cause performance problems on resource-limited workstations or on bandwidth-limited network links. Providing links to such images allows the user to select which larger images he or she wishes to see.	The execution of the IMA will be inspected to verify that large graphic images are not automatically downloaded to IMA web clients. Images larger than 50 Kbytes should not automatically downloaded.

The image size of 50 Kbytes should be used as guidance for determining which images should not be downloaded automatically.	

OPS-25 Web pages shall not contain background images.

REQUIREMENT CLARIFICATION	TEST METHOD
Background images that provide no additional functional value require additional bandwidth for transmission and may make overlaying text difficult to read. A background color may be selected; however, note that some sites permit only WHITE as a background color.	The execution of the IMA will be inspected to verify that images are not included in the backgrounds of IMA web pages.

3.5 USER INTERFACE

GUI-1 The IMA shall allocate read-only color cells from the default color map.

REQUIREMENT CLARIFICATION	TEST METHOD
Using color cells in the default color map, maintained by the X server, is suitable for most IMAs on Unix systems. Each IMA requests allocation of color cells in order to use the colors for its display. Color cells in the default color map can be allocated as read-only cells or read-write cells. Read-only cells do not permit changing of the color value once the cell has been initialized. Therefore, read-only cells can be shared by more than one IMA. Read-write cells permit changing the color value that is stored in the cell (i.e., the color can be changed.). The X11 architecture does not allow sharing of read-write color cells. When an IMA requests a color and specifies read-only, the X server returns either the identifier of a previously allocated read-only color cell that contains that color value or the identifier of a newly allocated read-only cell that has been initialized with that color value. In order to improve coexistence of applications, IMAs should use read-only color cells as a general rule. Doing so permits sharing of color cells among applications and prevents (or delays) exhaustion.	The default color map can be determined by executing the “xdpyinfo” command from a shell window. The color map used by an IMA can be determined by executing the “xwininfo” command for each window (or just the main window as appropriate) of the IMA. The ID number of the color map output from the "xwininfo" command should match the color map ID number output from the "xdpyinfo" command. The allocation of color cells can be observed using the “xcolor” utility. If all of the IMA’s color cells are read-only, then the number of allocated color cells should not increase after the IMA has been started the first time. The number of allocated color cells will subsequently increase only if read-write cells are requested by the IMA. Once the color cells have been completely allocated, the IMA under test is executed again. If there are not sufficient read-only color cells available, then the IMA will either terminate or display in a mix of color and black and white. This approach implies that the cells that are being shared or not shared have been allocated by previous processes of the same IMA. This may not be entirely reliable depending upon the number of color cells that were allocated prior to starting the first invocation of the IMA. However, it should provide some information about the types of color cells allocated to the IMA. This requirement is Not Applicable for the NT.

GUI-2 The IMA shall allocate a private color map in order to avoid filling the default color map with non-shared, read/write color cells.

REQUIREMENT CLARIFICATION	TEST METHOD
An IMA that requires a large number of read-write color cells may elect to use a private color map. This is an acceptable approach for such an IMA because it reduces the probability of other IMAs failing to execute because they cannot obtain their colors. Use of private color maps will cause color flashing on the display whenever the X server switches focus between a window associated with the default color map and a window that uses a different (i. e., private) color map.	The design documentation should identify the need and implementation of the private color map. "xdpyinfo" and "xwininfo" can be used to obtain the identifiers of the default and private color maps. In actual usage, color flashing will be observed when focus changes from a window using the default color to a window owned by the IMA under test that uses a private color map. Unlike X-11, the Windows NT architecture does allow the sharing of colors from it's color map. Although color flashing does occur in NT, it's effects are minimized due to the way Windows handles bitmaps and the dynamic reallocation of the color palette when an application is brought into focus. This requirement is Not Applicable for the NT.

GUI-3 The IMA shall display appropriate error messages when requested colors are not available.

REQUIREMENT CLARIFICATION	TEST METHOD
The X server returns an error to an IMA when a request for a color cannot be serviced because no read-only or free color cells are available. The IMA can either terminate or display the built-in black and white colors. If the IMA terminates, then the correct reason for termination (i.e., colors could not be obtained) must be displayed. The error message can be displayed in the console window or in a popup window if possible. Applications should also write an appropriate message to the IMA audit trail.	The default color map will be filled with a sufficient number of read-write color cells so that the IMA is unable to obtain all of its requested colors. This can be done using either a test driver that allocates read-write cells or by starting several invocations of an IMA that is known to use read-write cells. Once the color map is filled, the IMA is started. The display of a suitable error message that describes the reason (i.e., cannot allocate colors) for termination will be observed. If the IMA sends audits via the infrastructure audit Application Program Interface (API), the audit file will be examined for accompanying audit messages reporting the termination of the IMA and the reason for termination.

GUI-4 IMA windows shall provide panning or scrolling methods to view panes larger than the available frame.

REQUIREMENT CLARIFICATION	TEST METHOD
The IMA design should take into consideration the amount and dimensions of the information that will be displayed in IMA windows. Scrolling or panning methods should be provided for windows in which information output may either be too large to display completely or may scroll past before the user can read the window contents. An enhanced window design will place scroll bars on windows if they are resized so that the full output cannot be viewed. Allowing the user to resize the window to display the full contents is an unsatisfactory solution, since there may be times when the largest window size is insufficient to display all of the output. Also, scroll bars are an indication that there is more output; it is possible that a user may not recognize that a window should be resized to view the complete output. Conversely, the IMA design should not place scroll bars on windows when the scroll bars would serve no purpose.	The IMA will be exercised to examine IMA windows in which information output is displayed. The presence or absence of scrolling or panning methods will be observed and the suitability or need for scrolling or panning methods will be evaluated.

GUI-5 The IMA shall support cut and paste between windows.

REQUIREMENT CLARIFICATION	TEST METHOD
Meeting this objective provides a user the ability to reduce errors resulting from incorrect data entries. In addition, the ability to cut and paste between windows will save time during the installation and test process.	The IMA will be examined to determine if user is able to cut and paste between windows.

GUI-6 The IMA shall permit resizing of IMA windows.

REQUIREMENT CLARIFICATION	TEST METHOD
Window resizing can be useful to allow the user to customize the appearance of the desktop or to enlarge a window to display more information. The IMA design should permit resizing for windows for which resizing may be useful. Conversely, some windows (e.g., pop-up status windows and copyright windows) do not require the capability to resize.	The IMA will be exercised to examine the windows displayed by the IMA. The capability to resize each window will be observed and the suitability or need for resizing will be evaluated.

GUI-7 A hyperlink shall not navigate to itself.

REQUIREMENT CLARIFICATION	TEST METHOD
When a link is selected, the action is to load a new page that is either in the same IMA or in a different IMA. A link does not navigate to itself (i.e., to the top of the page in which the link appears). The link should not navigate to the same visible portion of a document (i.e., the link is visible on the user's screen); the link can navigate to a different portion of the same document, thus saving the user time to scroll down to that point. Each link on a page navigates to a different destination; the same link is not repeated with different names.	Links on the IMA home pages and on various sub-pages will be selected to verify that the current page is not the destination of the link. The objective is met if selecting any link does not result in the same viewable portion of a document being visible in the resulting displayed page.

GUI-8 A hyperlink in a web document that jumps to a destination outside the document shall identify its destination.

REQUIREMENT CLARIFICATION	TEST METHOD
Links that jump outside a document can be distracting since	Links on the IMA home pages and on selected sub-pages will be selected to

they draw attention to supplemental information that a user may not elect to view. Such links should be identified by name or description.	determine if a) the link is external and b) the destination of the link is explicitly identified.

3.6 SECURITY

SEC-1 The directories touched during the IMA installation shall not contain files or directories that are world-writeable as a result of installation of the IMA.

REQUIREMENT CLARIFICATION	TEST METHOD
The intent of this objective is to ensure that the installation of an IMA does not result in the presence of files or directories in the IMA directory tree that are world-writeable. This can happen inadvertently due to an incorrectly set umask or because of an incorrectly designed installation procedure. This objective cannot be met if there are world-writeable files or directories in the IMA directory tree that have consequences for either the security of the IMA or the security of the platform. It is also possible that some files or directories in the IMA's directory tree should be world-writeable. This is acceptable provided such files or directories do not introduce security vulnerabilities. These files and directories should be identified in the IMA installation and security documentation.	The following command can be used to scan the IMA directory tree for world-writeable files: Unix: *find root_dir -perm -0002 -print* NT: *perm root_dir* *root_dir* is the root of the IMA directory tree. The -perm option of -0002 will match all files and directories that are world-writeable. The print option will display each file or directory to the standard output. This command can be piped to the input of another command as necessary.

SEC-2 The IMA shall not require software development tools on functional user workstations.

REQUIREMENT CLARIFICATION	TEST METHOD

The presence or absence of software development tools on workstations or servers is a site security policy item. Development tools include tools that compile source code into executable objects, tools that interpret and execute source code files, and tools that are used to trace and debug an executing object. The intent of this requirement is to prevent users from modifying the intended behavior of an IMA and from introducing new executable objects onto a workstation. Compilers and compiler support software (e.g., the C and C++ compilers) are not permitted on general user workstations. The execution of compiled software objects does not require the presence of these tools. Compilers for mobile code such as Java are included in this group. Likewise, software debuggers are not needed to execute the IMA. A debugger might be used to modify the behavior of the IMA and should not be available on user workstations. Interpreter software, such as perl or tcl/tk, are necessary in order to launch and run software written in those languages. Any mission application software that includes interpreted software must be adequately protected from alteration. Development tools may be required on certain systems, such as development systems. The site security concept of operations must address this issue. However, functional users must not need them in order to use the IMA.	The IMA configuration and installation guide will be examined to verify that software development tools are not required to use the IMA. The IMA will be installed on workstations that are loaded with the standard DODIIS infrastructure that does not include software development tools. Following installation of the IMA, the directories that have been touched by the IMA installation will be examined to verify that no software development tools have been added to the workstation (e.g., C compilers). Tools that are not permitted on user systems include: - cc and other C compilers - c++ and other C++ compilers - dbx, adb, sdb, and other debuggers - Javac and other JAVA compilers Directories will be examined by executing the command: Unix: *ls -latR* NT: *dir ls* The presence of interpreters for perl, tcl/tk, or other scripting languages is acceptable. However, any mission application script that is interpreted and executed should be examined to ensure that its permissions do not permit unauthorized modification.

SEC-3 The IMA shall not implement or require storage of passwords in clear text.

REQUIREMENT CLARIFICATION	TEST METHOD

In order to simplify or speed up user access to IMA server applications, the IMA may implement storage of passwords for transmission to server applications. However, for obvious security reasons, these passwords must not be stored in clear text. This is particularly critical if general users can read the stored information without acquiring any additional privileges.	During installation and configuration of the IMA, the test engineer will verify that the IMA stores passwords for general users and identify the storage locations. The test engineer will examine the storage locations and view the passwords. The requirement is not met if the passwords are stored in clear text.

SEC-4 The IMA shall not require the presence of an entry relating to the IMA server in the /.rhosts file.

REQUIREMENT CLARIFICATION	TEST METHOD
Entries in the /.rhost should be made with care since several security vulnerabilities can be traced to incorrect usage of this file. Depending upon the site security architecture and the IMA design, an entry in the /.rhost file may be appropriate. However, using the /.rhost file is discouraged in most cases; therefore the entries should be kept to a minimum. Using the /.rhost file to permit transparent access by root from remote workstations should be avoided unless absolutely necessary. Instead, the access should be mapped to another user ID.	The /.rhosts file on the test workstation(s) will be examined for entries corresponding to the IMA server. If such entries are found, they will be removed to determine if IMA requires the deleted entries to function correctly. This requirement is Not Applicable for the NT, since there is no equivalent /.rhosts file.

SEC-5 The IMA shall use system access control facilities for discretionary access.

REQUIREMENT CLARIFICATION	TEST METHOD
In general, IMAs must rely on the security services provided by the DODIIS infrastructure instead of duplicating them. An IMA will only implement security functions that are unique to itself and that cannot be met by the infrastructure security services. The protection mechanisms of the	The appropriate IMA documentation, e.g., System Security Requirements, System Security Analysis, will be examined to determine the implementation of discretionary access by the IMA. Based upon the IMA design and implementation, ad hoc test cases will be

platform operating system are considered adequate and acceptable for discretionary access control (DAC). It is not necessary for an IMA to provide additional access control functions unless there are specific reasons, such as IMA level security, to do so. Application program managers must confirm such requirements and obtain approval from the DODIIS Engineering Review Board (ERB) and the IMA security certifier before implementing additional DAC.	run by the test team to exercise and demonstrate the discretionary access functions of the IMA.

SEC-6 The IMA shall not require users to login using privileged user accounts.

REQUIREMENT CLARIFICATION	TEST METHOD
General users must not need to login as root or as a privileged user (e.g., an administrative user on NT) to perform general user functions. While specific IMA functions may require execution with additional privileges, the privilege can be granted on demand by the IMA in a way that is transparent to the user. Additional privileges may be required to manage the IMA.. Users who perform management of the system's resources or who are responsible for the security of the system are the only individuals who should have access to root privileges or to other system privileges.	The appropriate IMA documentation (e.g., SDD, Software User's Manual (SUM)) will be examined to verify that login as root or as a privileged user is not required to use the IMA. The test engineer will login to the IMA as a general user, following the configuration and installation of the IMA. The test engineer will perform ad hoc tests to verify the basic function of the IMA.

SEC-7 The IMA shall not require functional user access to a shell.

REQUIREMENT CLARIFICATION	TEST METHOD
Although restriction of shell access is no longer considered a security requirement, uncontrolled use of the shell should be discouraged. This not only prevents users from taking	The appropriate IMA documentation (e.g., SUM) will be examined to identify how a user invokes and executes the IMA. The documentation will verify that shell access is not required to use the IMA. Following

advantage of vulnerabilities of the operating system or workstation configuration, but also reduces the possibility of users damaging either data or environment by incorrect usage of Unix operating system capabilities. Instead, user interaction with the IMA should be through graphical user interfaces.	configuration and installation of the IMA, invoke the IMA. Execute ad hoc test cases to verify that the IMA will execute properly without the use of a shell.

SEC-8 IMA programs shall not be setuid or setgid to another user ID or group ID.

REQUIREMENT CLARIFICATION	TEST METHOD
The "setuid" programs are a source of potential security vulnerabilities in site workstations and servers, particularly if the IMA provides to the user the capability (intended or unintended) to obtain a shell window. For most purposes, restricting IMA access by Unix group membership is a suitable and acceptable approach. The need to configure the IMA as a setuid program should be stated clearly in the IMA design documentation. Likewise, setgid (set groupid) programs also may provide security vulnerabilities, although to a lesser extent than setuid programs.	Following the configuration and installation of the IMA, the permissions that are set on the IMA executable files will be reviewed to verify that the setuid bits and/or the setgid bits are not set. For each file that has the setuid bit or the setgid bit set, the exact permissions will be noted. Setuid files that are not writeable by others do not meet this requirement, but will be assigned a lesser impact level than setuid files that are writeable by others. The same is true of setgid files that are not writeable by group members. Locate suid and sgid files by the following script: *cd <APPLICATION_ROOT>* *find . -perm -4000 -ls* *find . -perm -2000 -ls* The first command searches for files that are setuid. The second command searches for files that are setgid. The requirement is met if neither command reports any files. This requirement is Not Applicable for the NT.

SEC-9 The IMA shall not be used to modify operating system and other shared files.

REQUIREMENT CLARIFICATION	TEST METHOD
In general, execution of the IMA should not create security vulnerabilities for other IMAs or for the operating system of the user's workstation or of the platform on which the IMA server resides. Vulnerabilities could occur due to changes in permissions of IMA files, changes in ownership of IMA files or other files, or modification of the contents of IMA files and files shared with other IMAs. This objective applies to all phases of IMA usage, i.e., startup and initialization, information processing, logging/auditing, and IMA termination. This also includes the capability of obtaining a command line prompt (e.g., a UNIX shell) from within the application. While access to the command line may not be prohibited, it is a service of the infrastructure, not of the IMA, and such a capability might allow a user to modify resources without authorization.	The IMA documentation will be reviewed to determine the IMA files and other shared files that are referenced by the IMA during normal use. The requirement is not met if a file written by the IMA contains system-wide resource that would create security vulnerabilities for other IMAs or for the operating system of the user's workstation.

SEC-10 The IMA shall not implement audit collection or audit delivery functions.

REQUIREMENT CLARIFICATION	TEST METHOD
The DODIIS infrastructure provides an audit API for IMAs. IMAs that use this API do not have any need to implement additional audit functionality.	The appropriate IMA documentation (e.g., System Security Requirements, System Security Analysis) will be examined to determine the use of the infrastructure audit API for generating audit records. The IMA will be inspected to verify that audit collection or audit delivery functions are not implemented by the IMA.

SEC-11 The IMA shall use the infrastructure audit API for generating audit records.

REQUIREMENT CLARIFICATION	TEST METHOD

The DODIIS infrastructure provides a set of security functions. This set includes a single audit API for use by IMAs to write and transmit audit records. Therefore, there is no need for an IMA to either use a different audit mechanism or to implement its own unique audit mechanism.	The appropriate IMA documentation (e.g., System Security Requirements, System Security Analysis) will be examined to determine that audit API is being used for generating audit records by the IMA. **For UNIX:** To verify the use of the audit API for generating audit records by the IMA execute the following command in ashell window: *tail -f /var/log/syslog* Note: The lines are displayed in the window as IMAs and IMA utilities write them to the syslog file. Using selected test cases from the IMA security test procedures, verify that IMA audits are written to **/var/log/syslog** and are displayed to the shell window at the same time. The audit API generates audit records in the following format: ***DTG:Process Name [PID]:Program:Program Event ID:Message Level:User Name [UID]:Event Specific Information\n*** The *DTG* field consists of the month, day, and time the audit record was generated. The *Process Name [PID]* field is the ASCII name of the process that generates the message; the Process Identifier (PID) is placed within square brackets. The process name includes the name of the workstation or server on which the process is running. The *Program* field is the ASCII name of the project that generated the audit event The *Program Event ID* field is the numeric ID associated with the audit event.

	The *Message Level* field is an ASCII keyword that indicates the urgency level of the audit record. The *User Name [UID]* field contains the ASCII name and numeric user ID of the general user that owns the process generating the message. The *Event Specific Information* field is determined by the security requirements of the IMA and must be terminated with a new line character, '\n'. **For NT:** The Event Log is used to store audit information from an IMA. From the Start menu select: *Programs->Administrative Tools->Event Viewer* Once the window is displayed select: *Application from the Log menu* All applications Logs for are displayed.

SEC-12 The IMA audit strategy shall be integrated into site audit architecture.

REQUIREMENT CLARIFICATION	TEST METHOD
The use of the infrastructure audit interface is required. Compliance with this requirement is an important step toward integrating the IMA auditing into the site audit architecture. This is because all IMAs that comply with this requirement will be using the same audit (API) and the same audit formats. This uniformity will improve the ability of a site to implement a single approach to audit collection and	The primary consideration in evaluating if an IMA meets this objective is the level of effort required to integrate the IMA's audit into a site's audit architecture. A strategy that does not use either the infrastructure audit API or the operating system audit API does not meet this objective. Reliance on the operating system API can pose difficulties since the audit API and audit format will differ across the operating systems. Since the operating system audits must also be integrated into the site audit architecture, this approach

analysis. A site's audit strategy will also include collection and analysis of operating system audit data. An IMA may either rely on the operating system auditing or actually generate audits that use the operating system audit API. The approach should be clearly documented in the IMA design documentation, and the audit collection mechanism, API, and audit formats should be clearly described.	acceptable. However, it poses a level of effort that is higher than the use of the audit API.

SEC-13 The IMA web server shall audit user activity in accordance with DODIIS security policy.

REQUIREMENT CLARIFICATION	TEST METHOD
IMA web servers must provide audit records of user activity. This is important since the user's workstation will not provide information on activity that occurs during browser sessions. Audit records should include, at a minimum, the requesting host, date and time, username, web page and/or data accessed, and type of operation (read, write, etc.).	IMA documentation will be reviewed to identify the auditing strategy of the IMA web server. The IMA will be exercised from a client workstation. The audit trail of the IMA server will be monitored to verify that the IMA server is auditing user activity. If the IMA does not use a web server this requirement is Not Applicable.

SEC-14 The IMA web server shall not store sensitive information in cookies.

REQUIREMENT CLARIFICATION	TEST METHOD
Although security policy does not prevent the use of cookies, an IMA should not write sensitive information to the cookie file. Sensitive information is any information, such as the user's password, that may affect the security posture of the IMA or of other site systems.	The IMA will be exercised from a client workstation. The browser in use on the workstation will be configured to accept cookies. During the user's session with the IMA server, the browser cookie file will be monitored and the contents of each cookie written by the browser will be examined for potential vulnerabilities.

	If the IMA does not use a web server this requirement is Not Applicable.

SEC-15 If the IMA web server implements identification and authentication, then browser access to pages on the server by explicit URL addressing shall be denied unless the user has already been authenticated.

REQUIREMENT CLARIFICATION	TEST METHOD
IMA web servers may implement login as part of the IMA identification and authentication policy. In order to use the IMA, the user accesses the server via a browser. The initial web page requires the user to entire an identifier and password before he or she is allowed to use the IMA. For such an implementation, the user must not be permitted to access pages on the server by entering an absolute path to a document or service in the browser destination field. An attempt like this can be used to bypass the identification and authentication mechanism of the IMA and should either be denied or mapped to the IMA login window.	The IMA will be exercised from a client workstation. The test engineer will collect absolute paths to documents or directories that are available on the IMA server. Prior to logging in to the IMA, the test engineer will enter absolute paths in the destination field of the browser. The objective is met if each attempt to use the absolute path is either denied or the test engineer is presented the IMA login page. If the IMA does not use a web server this requirement is Not Applicable.

4. APPENDIX A

DODIIS Integration Checklist

This appendix provides a summary listing of the DODIIS integration requirements. The following table lists each requirement. The numbering of the integration requirements has changed from the previous version. For the purpose of continuity, each requirement is mapped to its corresponding requirement in the previous version of the integration specifications. The source document in which the original requirement was stated is provided as an additional reference.

Several new requirements have been added. These requirements address elements of DODIIS architecture that have not been covered in the earlier versions of the integration requirements (e.g., browser-based architecture). The requirements are derived from both accepted technical practices and conventions and from the expertise and knowledge that has been acquired by the JITF during integration testing.

No reference documents are provided for the new requirements.

The following documents are reference documents for the integration requirements.

Test Procedures Volume 1 -- *Joint Integration Test Facility (JITF) Test Procedures, Volume 1, Infrastructure Compliance Testing*, 18 June 1997.

Test Procedures Volume 2 -- *Joint Integration Test Facility (JITF) Test Procedures, Volume 2, Installation and Integration Scenario Testing*, 18 June 1997.

CSE Integration -- *DODIIS CSE Integration Objectives And Evaluation Procedures DRAFT* 2, October 1996.

User Interface Spec -- *User Interface Specifications for the Defense Information Infrastructure (DII) Version 3.0*, February 1998.

DODIIS Instructions -- *DODIIS Instructions,* April 1999.

REQUIREMENT	REFERENCE	REFERENCE DOCUMENT
DOCUMENTATION		
DOC-1 IMA documents shall contain page numbers for all sections and appendices.	DOC-1	TEST PROCEDURES 2.0
DOC-2 IMA documents shall contain numbered sections.	DOC-2	TEST PROCEDURES 2.0

REQUIREMENT	REFERENCE	REFERENCE DOCUMENT
DOC-3 Figures and tables in IMA documents shall have titles and reference numbers.	NEW	
DOC-4 Soft copy documents shall match hard copy versions in content, structure, and sectioning.	DOC-3	TEST PROCEDURES 2.0
DOC-5 IMA configuration and installation information shall be consolidated into a single configuration and installation document.	DOC-5	TEST PROCEDURES 2.0
DOC-6 The IMA configuration and installation guide shall include installation verification information.	DOC-6	TEST PROCEDURES 2.0
DOC-7 The IMA configuration and installation guide shall specify if the IMA requires a dedicated platform for the IMA server or if the IMA server can be installed on a platform shared with other IMA servers.	DOC-7	TEST PROCEDURES 2.0
DOC-8 The IMA installation and configuration guide shall contain step by step instructions to perform IMA installation and configuration.	DOC-8	TEST PROCEDURES 2.0
DOC-9 IMA configuration and installation guide shall include instructions to add the IMA to the infrastructure application selection mechanism.	DOC-9	TEST PROCEDURES
DOC-10 IMA documentation shall specify points of contact (phone, electronic mail, etc.) for IMA support.	DOC-11	
DOC-11 The IMA configuration and installation guide shall specify the minimum amount of disk space needed to install and execute the IMA.	DOC-12	TEST PROCEDURES 2.0

REQUIREMENT	REFERENCE	REFERENCE DOCUMENT
DOC-12 The IMA configuration and installation guide shall specify the name(s) and size(s) of file system(s) that are required to install and execute the IMA.	DOC-13	TEST PROCEDURES 2.0
DOC-13 The IMA configuration and installation guide shall specify the recommended and minimum size of random access memory (RAM) required to execute the IMA.	DOC-14	TEST PROCEDURES 2.0
DOC-14 The IMA configuration and installation guide shall specify the operating system versions and operating system packages/subsets that must be installed to support the IMA.	DOC-15	TEST PROCEDURES 2.0
DOC-15 The IMA configuration and installation guide shall specify the operating system patch levels that must be installed to support the IMA.	DOC-16	TEST PROCEDURES 2.0
DOC-16 The IMA configuration and installation guide shall specify any modifications made to the operating system configuration that are required to support the IMA.	DOC-17	TEST PROCEDURES 2.0
DOC-17 The IMA configuration and installation guide shall specify additional hardware and associated drivers that are required to support the IMA.	DOC-18	TEST PROCEDURES 2.0
DOC-18 The IMA configuration and installation guide shall specify additions/modifications to system configuration files that are required to support the IMA.	DOC-19	TEST PROCEDURES 2.0

REQUIREMENT	REFERENCE	REFERENCE DOCUMENT
DOC-19 The IMA configuration and installation guide shall provide rules defining appropriate file ownerships and permissions for all files and directories that are loaded or modified during IMA installation.	DOC-20	TEST PROCEDURES 2.0
DOC-20 The IMA configuration and installation guide shall specify the audit configurations (i.e., audit flags, etc.) that must be set in order to meet the system security requirements.	DOC-21	TEST PROCEDURES 2.0
DOC-21 The IMA configuration and installation guide shall identify other software products on which the normal operation of the IMA is dependent.	DOC-22	TEST PROCEDURES 2.0
DOC-22 Comprehensive instructions shall be provided for uninstalling the IMA, including backing out of a failed installation so that it can be reinstalled.	DOC-23	TEST PROCEDURES 2.0
DOC-23 IMA documentation shall specify the browsers and browser versions that are compatible with the IMA.	DOC-24	TEST PROCEDURES 2.0
DOC-24 IMA configuration and installation guide shall specify any browser settings that are necessary to access the IMA.	DOC-25	TEST PROCEDURES 2.0
DOC-25 If the IMA design requires the use of plug-ins, the IMA documentation shall include a list of required browser plug-ins, the source of the plug-ins and appropriate licenses, and DMB approval to use the plug-ins.	DOC-26	TEST PROCEDURES 2.0

REQUIREMENT	REFERENCE	REFERENCE DOCUMENT
DOC-26 If the IMA design includes implementation of JAVA applets, the IMA documentation shall include documentation of IMA server registration with Intelink Central, documentation of JAVA applet registration with Intelink Central, and documentation of results of JAVA applet code review.	DOC-27	TEST PROCEDURES 2.0
DOC-27 IMA configuration and installation guide shall specify the network address and port number for proxy server(s) if required to access the IMA web server.	DOC-28	TEST PROCEDURES 2.0
DOC-28 IMA documentation shall specify Uniform Resource Locator (URL) for access to the IMA as a logical hostname that can be resolved by the site's name resolution service.	DOC-29	TEST PROCEDURES 2.0
DOC-29 IMA design documentation shall specify if secure HTTPS connections are required.	DOC-30	TEST PROCEDURES 2.0
DOC-30 IMA design documentation shall specify the standards implemented by the IMA that are mandated by the Joint Technical Architecture (JTA).	NEW	
INSTALLATION AND CONFIGURATION		
INST-1 IMA installation shall not require installation of the operating system.	INST-1	TEST PROCEDURES 2.0
INST-2 IMA installation shall not require reinstallation of currently loaded COTS or GOTS applications.	INST-2	TEST PROCEDURES 2.0
INST-3 The IMA shall not include bundled support applications.	INST-3	TEST PROCEDURES 2.0
INST-4 The IMA shall not include bundled implementations of any standard network protocol.	INST-5	TEST PROCEDURES 2.0

REQUIREMENT	REFERENCE	REFERENCE DOCUMENT
INST-5 IMA installation design shall support installation on user workstations and applications servers for export to user workstations.	INST-4	TEST PROCEDURES 2.0
INST-6 IMA shall not modify the native programming utilities and libraries.	INST-6	TEST PROCEDURES 2.0
INST-7 IMA shall not require modification of networking protocols or services.	INST-7	TEST PROCEDURES 2.0
INST-8 The IMA software and documentation shall explicitly identify the software version and release of IMA in both documentation and software.	INST-8	TEST PROCEDURES 2.0
INST-9 The IMA can be un-installed using instructions provided in the IMA configuration and installation guide.	INST-9	TEST PROCEDURES 2.0
INST-10 The IMA installer shall not be required to make changes to installation scripts as part of the installation process.	INST-11	TEST PROCEDURES 2.0
INST-11 The IMA system installer shall not be required to enter extraneous or superfluous information during installation.	INST-10	TEST PROCEDURES 2.0
INST-12 Manual input for configuration and installation shall be limited to responding to prompts and/or editing configuration file(s) and shall not involve entering information that the script can obtain automatically.	INST-12	TEST PROCEDURES 2.0
INST-13 The initial configuration and installation parameters shall be consistently set across the software components comprising the IMA.	INST-13	TEST PROCEDURES 2.0
INST-14 IMA shall not reserve an explicit group identifier (ID) or user ID on Unix platforms or a specific user/group on NT platforms.	INST-14	TEST PROCEDURES 2.0

REQUIREMENT	REFERENCE	REFERENCE DOCUMENT
INST-15 IMA shall not bundle Commercial Off-The-Shelf (COTS) or Government Off-The-Shelf (GOTS) software in its directory tree.	INST-15	TEST PROCEDURES 2.0
INST-16 Installation of the IMA shall not replace resources that are used by other IMAs.	INST-16	TEST PROCEDURES 2.0
INST-17 IMA shall not overwrite or replace the native RPC map.	INST-17	TEST PROCEDURES 2.0
INST-18 The IMA shall not require secure Network File System (NFS).	INST-18	TEST PROCEDURES 2.0
INST-19 IMA files shall be contained in **/opt/IMA_name** or **/opt/hostname#/IMA_name**.	INST-19	TEST PROCEDURES 2.0
INST-20 IMA shall only use colors defined in the standard color data base.	INST-20	TEST PROCEDURES 2.0
INST-21 IMA shall use only fonts from the platform's native font set.	INST-21	TEST PROCEDURES 2.0
INST-22 The IMA shall not require specific settings of permissions and ownership of browser files and directories.	INST-23	TEST PROCEDURES 2.0
INST-23 Installation of the IMA client shall not modify the home page settings of users.	INST-24	TEST PROCEDURES 2.0
INST-24 Installation of the IMA client shall not overwrite or modify default browser configuration settings of any user.	INST-25	TEST PROCEDURES 2.0
INST-25 Installation of the IMA client shall not require modification of the user's mail and news configuration.	INST-26	TEST PROCEDURES 2.0
INST-26 The HTTP server directory structure shall be separate from the HTML documents directory.	INST-27	TEST PROCEDURES 2.0
INST-27 An "index.html" or equivalent file shall be used to control default web pages.	INST-28	TEST PROCEDURES 2.0
INST-28 All URLs referenced in HTML links shall contain at least one '.'.	INST-29	TEST PROCEDURES 2.0

REQUIREMENT	REFERENCE	REFERENCE DOCUMENT
INST-29 The "httpd" and any IMA required daemons shall be started automatically when the server boots to multi-user mode.	INST-30	TEST PROCEDURES 2.0
INST-30 The web server shall log all connections and data requests that are received by the httpd daemon.	INST-31	TEST PROCEDURES 2.0
INST-31 The web server configuration shall implement Discretionary Access Control (DAC).	NEW	
INST-32 The httpd daemon shall be owned and run by a user name that is not superuser (Unix) or an administrative user (NT).	INST-34	TEST PROCEDURES 2.0
INST-33 Web IMA file names shall use appropriate file name extension for the content type.	INST-35	TEST PROCEDURES 2.0
INST-34 Readme files and errata sheets shall contain only last minute and errata type information that could not be incorporated into the final printing of the official configuration and installation guide.	DOC-4	TEST PROCEDURES 2.0
INST-35 The media delivered by the PMO to the JITF will include only the baseline for the release version under test.	NEW	
INST-36 The installation and configuration of the IMA shall be completed in 20 working hours.	NEW	
INST-37 The IMA design shall not prohibit installation and operation of the application on a platform shared by other applications.	NEW	
ENVIRONMENT		
ENV-1 The IMA shall not modify system files in any way that causes the computing platform to fail to boot if the IMA client or IMA server is unavailable.	ENV-1	TEST PROCEDURES 2.0

REQUIREMENT	REFERENCE	REFERENCE DOCUMENT
ENV-2 Execution of the IMA shall not replace or alter system resources that are used by other IMAs.	ENV-2	TEST PROCEDURES 2.0
ENV-3 The IMA shall not prevent or alter login if the IMA server or client is unavailable.	ENV-3	TEST PROCEDURES 2.0
ENV-4 The client application(s) of the IMA shall launch from the background menu or from an icon on the desktop.	ENV-4	TEST PROCEDURES 2.0
ENV-5 The server application(s) of the IMA shall not require manual launching by an administrator.	NEW	
ENV-6 IMA environment variables shall be defined in the form of PRODUCT_VARNAME.	ENV-5	TEST PROCEDURES 2.0
ENV-7 IMA shall use the directory defined by the TMPDIR environment variable for all temporary files.	ENV-6	TEST PROCEDURES 2.0
OPERATION		
OPS-1 IMA file names shall consist of valid characters for file names and shall be restricted to the maximum length of 128 chars for UNIX/Solaris systems and 255 chars for Windows NT systems.	OPS-1	TEST PROCEDURES 2.0
OPS-2 The IMA shall use the platform's native keyboard map.	OPS-2	TEST PROCEDURES 2.0
OPS-3 The execution environment that exists at the time of IMA launch shall not conflict with either the user's overall operating environment or the execution environment of other applications.	OPS-3	TEST PROCEDURES 2.0

REQUIREMENT	REFERENCE	REFERENCE DOCUMENT
OPS-4 The IMA shall not contain configuration files or tables that duplicate information already contained in the operating system configuration files.	OPS-4	TEST PROCEDURES 2.0
OPS-5 IMA shall not use extensions to the Window System (X or Windows NT) that are not supported by the infrastructure.	OPS-5	TEST PROCEDURES 2.0

OPS-6 IMA shall use the infrastructure print utility for printing hard copy.	OPS-6	TEST PROCEDURES 2.0
OPS-7 Administration of the IMA shall not require access to privileged user accounts.	OPS-7	TEST PROCEDURES 2.0
OPS-8 The administrator shall be provided with utilities and tools to add, modify, or delete IMA users.	OPS-8	TEST PROCEDURES 2.0
OPS-9 The IMA shall use infrastructure management utilities to manage and distribute IMA, user, and security data.	OPS-9	TEST PROCEDURES 2.0
OPS-10 IMA files that "grow" as a result of IMA execution shall not fill or result in exhausted file system space.	OPS-10	TEST PROCEDURES 2.0
OPS-11 The loss of connectivity between the IMA client process and the IMA server process shall not affect the behavior or operation of other client workstation applications or utilities.	OPS-11	TEST PROCEDURES 2.0
OPS-12 Disorderly termination of the IMA shall not affect the execution or behavior of other applications.	OPS-12	TEST PROCEDURES 2.0
OPS-13 Disorderly termination of the IMA shall not result in incorrect behavior of the IMA when the IMA is restarted.	OPS-13	TEST PROCEDURES 2.0
OPS-14 Orderly termination of the IMA shall not affect the execution or behavior of other applications.	OPS-14	TEST PROCEDURES 2.0
OPS-15 Disorderly shutdown of the client workstation while the IMA is executing shall not affect the behavior or operation of the IMA on other workstations.	OPS-15	TEST PROCEDURES 2.0
OPS-16 Disorderly shutdown of the client workstation while the IMA is	OPS-16	TEST PROCEDURES 2.0

executing shall not result in incorrect behavior of the IMA when the IMA is restarted.		
OPS-17 User log out of the client workstation while the IMA is executing shall not affect the behavior of the IMA or the behavior of other applications in the user's next login session.	OPS-17	TEST PROCEDURES 2.0
OPS-18 The IMA shall exhibit consistent behavior across all supported operating systems and platforms.	OPS-18	TEST PROCEDURES 2.0
OPS-19 IMA shall not duplicate functions provided by support applications.	OPS-19	TEST PROCEDURES 2.0
OPS-20 IMA shall use shared libraries for UNIX/Solaris and DLL's for Windows NT.	OPS-20	TEST PROCEDURES 2.0
OPS-21 IMA shall not require use of a browser with acceptance of cookies enabled.	OPS-21	TEST PROCEDURES 2.0
OPS-22 Web pages shall not contain animations and animated GIF files that do not implement mission functions..	OPS-22	TEST PROCEDURES 2.0
OPS-23 Web pages shall not contain elements that obscure or interfere with reading clarity.	OPS-23	TEST PROCEDURES 2.0
OPS-24 Large graphic images shall be downloaded on demand. A small icon of the image shall be displayed on the web page and linked directly to the full-sized image.	OPS-24	TEST PROCEDURES 2.0
OPS-25 Web pages shall not contain background images.	OPS-25	TEST PROCEDURES 2.0
USER INTERFACE		

GUI-1 The IMA shall allocate read-only color cells from the default color map.	GUI-1	TEST PROCEDURES 2.0
GUI-2 The IMA shall allocate a private color map in order to avoid filling the default color map with non-shared, read/write color cells.	GUI-2	TEST PROCEDURES 2.0
GUI-3 The IMA shall display appropriate error messages when requested colors are not available.	GUI-3	TEST PROCEDURES 2.0

GUI-4 IMA windows will provide panning or scrolling methods to view panes larger than the available frame.	GUI-4	TEST PROCEDURES 2.0
GUI-5 The IMA shall support cut and paste between windows.	GUI-5	TEST PROCEDURES 2.0
GUI-6 The IMA shall permit resizing of IMA windows.	GUI-6	TEST PROCEDURES 2.0
GUI-7 A hyperlink shall not navigate to itself.	GUI-7	TEST PROCEDURES 2.0
GUI-8 A hyperlink in a web document that jumps to a destination outside the document shall identify its destination.	GUI-8	TEST PROCEDURES 2.0
SECURITY		
SEC-1 The directories touched during the IMA installation shall not contain files or directories that are world-writeable as a result of installation of the IMA.	SEC-1	TEST PROCEDURES 2.0
SEC-2 The IMA shall not require software development tools on functional user workstations.	SEC-2	TEST PROCEDURES 2.0
SEC-3 The IMA shall not implement or require storage of passwords in clear text.	NEW	
SEC-4 The IMA shall not require the presence of an entry relating to the IMA server in the /.rhosts file.	SEC-3	TEST PROCEDURES 2.0
SEC-5 The IMA shall use system access control facilities for discretionary access.	SEC-4	TEST PROCEDURES 2.0
SEC-6 The IMA shall not require users to login using privileged user accounts.	SEC-5	TEST PROCEDURES 2.0
SEC-7 The IMA shall not require functional user access to a shell.	SEC-6	TEST PROCEDURES 2.0

SEC-8 IMA programs shall not be setuid or setgid to another user ID or group ID.	SEC-7	TEST PROCEDURES 2.0
SEC-9 The IMA shall not be used to modify operating system and other shared files.	SEC-8	TEST PROCEDURES 2.0
SEC-10 The IMA shall not implement audit collection or audit delivery functions.	SEC-9	TEST PROCEDURES 2.0
SEC-11 The IMA shall use the infrastructure audit API for generating audit records.	SEC-10	TEST PROCEDURES 2.0
SEC-12 The IMA audit strategy shall be integrated into site audit architecture.	SEC-11	TEST PROCEDURES 2.0
SEC-13 IMA web server shall audit user activity in accordance with DODIIS security policy.	SEC-12	TEST PROCEDURES 2.0
SEC-14 IMA web server shall not store sensitive information in cookies.	SEC-13	TEST PROCEDURES 2.0
SEC-15 If the IMA web server implements identification and authentication, then browser access to pages on the server by explicit URL addressing shall be denied unless the user has already been authenticated.	SEC-14	TEST PROCEDURES 2.0

5. APPENDIX B - ACRONYMS

ACRONYM	DEFINITION
AIS	Automated Information System
API	Application Program Interface
COTS	Commercial Off-The-Shelf
CSE	Client Server Environment

CSE-SS	Client Server Environment System-Services
DBMS	Data Base Management System
DII COE	Defense Information Infrastructure Common Operating Environment
DMB	DODIIS Management Board
DODIIS	Department of Defense Intelligence Information System
ERB	Engineering Review Board
GIF	Graphics Interchange Format
GOTS	Government Off-The-Shelf
GUI	Graphical User Interface
html	Hyper Text Markup Language
http	Hyper Text Transfer Protocol
ID	Identifier
IP	Internet Protocol
IMA	Intelligence Mission Application
JITF	Joint Integration Test Facility
NFS	Network File System
NIS	Network Information Service
PID	Process Identifier
PMO	Program Management Office
RPC	Remote Procedure Call
SASS	System Acquisition Support Services
SDD	Software Design Document
SUM	Software User's Manual
TAR	Tape Archive
TCP	Transmission Control Protocol
TFUG	Trusted Facility User's Guide

URL	Uniform Resource Locator
VDD	Version Description Document
VTF	Virtual Test Folder
XPG	X/OPEN Portability Guide